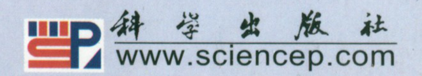
数学机械化丛书

数学机械化

吴文俊 著





中国科学院科学出版基金资助出版

《数学机械化丛书》获国家基础研究发展规划项目“数学机械化与自动推理平台”与“数学机械化应用推广专项经费”资助

数学机械化丛书

数学机械化

吴文俊 著

科学出版社

北京

内 容 简 介

本书是围绕作者命名的"数学机械化"这一中心议题而陆续发表的一系列论文的综述。本书试图以构造性与算法化的方式来研究数学，使数学推理机械化以至于自动化，由此减轻繁琐的脑力劳动。

全书分成三个部分：第一部分考虑数学机械化的发展历史，特别强调在古代中国的发展历史。第二部分给出求解多项式方程组所依据的基本原理与特征列方法。作为这一方法的基础，本书还论述了构造性代数几何中的若干问题。第三部分给出了特征列方法在几何定理证明与发现、机器人、天体力学、全局优化和计算机辅助设计等领域中的应用。

本书可供数学工作者，数学及计算机专业高年级大学生和研究生以及有关工程人员参阅。

图书在版编目(CIP)数据

数学机械化/吴文俊著．—北京：科学出版社，2003.3
(数学机械化丛书/吴文俊主编)
ISBN 7-03-010764-0

Ⅰ．数… Ⅱ．吴… Ⅲ．数学理论-计算机辅助计算 Ⅳ．O1-1

中国版本图书馆 CIP 数据核字(2002)第 063341 号

责任编辑：吕 虹 / 责任校对：柏连海
责任印制：安春生 / 封面设计：黄华斌

科学出版社 出版
北京东黄城根北街16号
邮政编码：100717
http://www.sciencep.com
双青印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2003 年 3 月第 一 版 开本：B5(720×1000)
2003 年 3 月第一次印刷 印张：25
印数：1—2 500 字数：466 000

定价：58.00 元

(如有印装质量问题，我社负责调换〈新欣〉)

《数学机械化丛书》前言[①]

十六七世纪以来，人类历史上经历了一场史无前例的技术革命，出现了各种类型的机器，取代各种形式的体力劳动，使人类进入一个新时代. 几百年后的今天，电子计算机已可以有条件地代替一部分特定的脑力劳动，因而人类面临另一场更宏伟的技术革命，处在又一个新时代的前夕. 数学是一种典型的脑力劳动，它在这一场新的技术革命中，无疑地将扮演一个重要的角色. 为了了解数学在当前这场革命中所扮演的角色，应对机器的作用，以及作为数学的脑力劳动的方式，进行一定的分析.

1. 什么是数学的机械化

不论是机器代替体力劳动，或是计算机代替某种脑力劳动，其所以成为可能，关键在于所需代替的劳动已经“机械化”，也就是说已实现了刻板化或规格化. 正因为割麦、刈草、纺纱织布的动作已经是机械化刻板化了的，因而可据此造出割麦机、刈草机、纺纱机织布机来. 也正因为加减乘除开方等运算这一类脑力劳动，几千年来就已经是机械地刻板地进行的，才有可能使得 17 世纪的法国数学家帕斯卡，利用齿轮传动造出了第一台机械计算机 —— 加法机，并由莱布尼茨改进成为也能进行乘法的机器. 数学问题的机械化，就要求在运算或证明过程中，每前进一步之后，都有一个确定的、必须选择的下一步，这样沿着一条有规律的、刻板的道路，一直达到结论.

在中小学数学的范围里，就有着不少已经机械化了的课题. 除了四则、开方等运算外，解线性联立方程组就是一个很好的例子. 在中学用的数学课本中，往往介绍解线性方程组的各种“消去法”，其求解过程是一个按一定程序进行的计算过程，也就是一种机械的、刻板的过程. 根据这一过程编成程序，由电子计算机付诸实施，就可以不仅机器化而且达到自动化，在几分钟甚至几秒钟之内求出一个未知数多至上百个的线性方程组的解答来，这在手工计算

---

① 20 世纪七八十年代之交，我尝试用计算机证明几何定理取得成功，由此并提出了数学机械化的设想. 先后在一些通俗报告与写作中，解释数学机械化的意义与前景，例如 1978 年发表于《自然辩证法通讯》的“数学机械化问题”以及 1980 年发表于《百科知识》的“数学的机械化”. 二文都重载于 1995 年由山东教育出版社出版的《吴文俊论数学机械化》一书. 经过 20 多年众多学者的努力，数学机械化在各个方面都取得了丰富多彩的成就，并已出版了多种专著，汇集成现在的数学机械化丛书. 现据 1980 年的《百科知识》的“数学的机械化”一文，稍加修改并作增补，以代丛书前言.

几乎是不可能的. 如果用手工计算, 即使是解只有三四个未知数的方程组, 也将是繁琐而令人厌烦的. 现代化的国防、经济建设中, 大量出现的例如网络一类的问题, 往往可归结为求解很多未知数的线性方程组. 这使得已经机械化了的线性方程组解法在四个现代化中起着一种重要作用.

即使是不专门研究数学的人们, 也大都知道, 数学的脑力劳动有两种主要形式: 数值计算与定理证明 (或许还应包括公式推导, 但这终究是次要的). 著名的数理逻辑学家美国洛克菲勒大学教授王浩先生在一篇有名的《向机械化数学前进》的文章中, 曾列举了这两种数学脑力劳动的若干不同之点. 我们可以简略而概括地把它们对比一下:

计　算	证　明
易	难
繁	简
刻板	灵活
枯燥	美妙

计算, 如已经提到过的加减乘除开方与解线性方程组, 其所以虽繁而易, 根本原因正在于它已经机械化. 而证明的巧而难, 是大家都深有体会的, 其根本原因也正在于它并没有机械化. 例如, 我们在中学初等几何定理的证明中, 就经常要依靠诸如直观、洞察、经验, 以及其他一些模糊不清的原则, 去寻找捷径.

2. 从证明的机械化到机器证明

一个值得提出的问题是: 定理的证明是不是也能像计算那样机械化, 因而把巧而难的证明, 化为计算那样虽繁而易的劳动呢? 事实上, 这一证明机械化的设想, 并不始自今日, 它早就为 17 世纪时的大哲学家、大思想家和大数学家笛卡儿和莱布尼茨所具有. 只是直到 19 世纪末, 希尔伯特 (德国数学家, 1862~1943) 等创立并发展了数理逻辑以来, 这一设想才有了明确的数学形式. 又由于 20 世纪 40 年代电子计算机的出现, 才使这一设想的实现有了现实可能性.

从 20 世纪二三十年代以来, 数理逻辑学家们对于定理证明机械化的可能性, 进行了大量的理论探讨, 他们的结果大都是否定的. 例如哥德尔 (Gödel) 等的一条著名定理就说, 即使看来最简单的初等数论这一范围, 它的定理证明的机械化也是不可能的. 另一方面, 1950 年波兰数学家塔斯基 (Tarski) 则证明了初等几何 (以及初等代数) 这一范围的定理证明, 却是可以机械化的. 只

是塔斯基的结果近于例外，在初等几何及初等代数以外的大量结果都是反面的，即机械化是不可能的．1956 年以来美国开始了利用电子计算机做证明定理的尝试．1959 年王浩先生设计了一个机械化方法，用计算机证明了罗素等著的《数学原理》这一经典著作中的几百条定理，只用了 9 分钟，在数学与数理逻辑学界引起了轰动．一时间，机器证明的前景似乎非常乐观．例如 1958 年时就有人曾经预测：在 10 年之内计算机将发现并证明一个重要的数学新定理．还有人认为，如果这样，则不仅许多著名哲学家与数学家，如皮亚诺、怀特海、罗素、希尔伯特以及图灵等人的梦想得以实现，而且计算将成为科学的皇后，人类的主人！

然而，事情的发展却并不如预期那样美好．尽管在 1976 年，美国的哈肯等人，在高速计算机上用了 1200 小时的计算时间，解决了数学家们 100 多年来所未能解决的一个著名难题 —— 四色问题，因此而轰动一时，但是，这只能说明计算机作为定理证明的辅助工具有着巨大潜力，还不能认为这样的证明就是一种真正的机器证明．用王浩先生的说法，哈肯等关于四色定理的证明是一种使用计算机的特例机证，它只适用于四色这一特殊的定理，这与所谓基础机器证明之能适用于一类定理者有别．后者才真正体现了机械化定理证明，进而实现机器证明的实质．另一面，在真正的机械化证明方面，虽然塔斯基在理论上早已证明了初等几何的定理证明是能机械化的，还提出了据以造判定机也即是证明机的设想，但实际上他的机械化方法非常繁，繁到不可收拾，因而远远不是切实可行的．1976 年，美国做了许多在计算机上证明定理的实验，在塔斯基的初等几何范围内，用计算机所能证明的只是一些近于同义反复的“儿戏式”的“定理”．因此，有些专家曾经发出过这样悲观的论调：如果专依靠机器，则再过 100 年也未必能证明出多少有意义的新定理来．

3. 一条切实可行的道路

1976 年冬，我们开始了定理证明机械化的研究．1977 年春取得了初步成果，证明初等几何主要一类定理的证明可以机械化．在理论上说来，我们的结果已包括在塔斯基的定理之中．但与塔斯基的结果不同，我们的机械化方法是切实可行的，即使用手算，依据机械化的方法逐步进行，虽然繁复，也可以证明一些艰深的定理．

我们的方法主要分两步，第一步是引进坐标，然后把需证定理中的假设与终结部分都用坐标间的代数关系来表示．我们所考虑的定理局限于这些代数

关系都是多项式等式关系的范围, 例如平行、垂直、相交、距离等关系都是如此. 这一步可以叫做几何的代数化. 第二步是通过代表假设的多项式关系把终结多项式中的坐标逐个消去, 如果消去的结果为零, 即表明定理正确, 否则再作进一步检查. 这一步完全是代数的, 即用多项式的消元法来验证.

上述两步都可以机械与刻板地进行. 根据我们的机械化方法编成程序, 以在计算机上实现机器证明, 并无实质上的困难. 事实上中国科学院数学研究所某些同志以及国外的王浩先生都曾在计算机上试行过. 我们自己也曾在国产的长城 203 台式机上证明了像西摩松线那样不算简单的定理. 1978 年初我们又证明了初等微分几何中主要的一类定理证明也可以机械化. 而且这种机械化方法也是切实可行的, 并据此用手算证明了不算简单的一些定理.

从我们的工作中可以看出, 定理的机械化证明, 往往极度繁复, 与通常既简且妙的证明形成对照, 这种以量的复杂来换取质的困难, 正是利用计算机所需要的.

在电子计算机如此发展的今天, 把我们的机械化方法在计算机上实现不仅不难, 而且有一台微型的台式机也就够了. 就像我们曾经使用过的长城 203, 它的存数最多只能到 234 个 10 进位的 12 位数, 就已能用以证明西摩松线那样的定理. 随着超大规模集成电路与其他技术的出现与改进, 微型机将愈来愈小型化而内存却愈来愈大, 功能愈来愈多, 自动化的程度也愈来愈高. 进入 21 世纪以后, 这一类方便的小型机器将为广大群众普遍使用. 它们不仅将成为证明一些不很简单的定理的武器, 而且还可用以发现并证明一些艰深的定理, 而这种定理的发现与证明, 在数学研究手工业式的过去, 将是不可想象的. 这里我们应该着重指出, 我们并不鼓励以后人们将使用计算机来证明甚至发现一些有趣的几何定理. 恰恰相反, 我们希望人们不再从事这种虽然有趣却对数学甚至几何学本身也已意义不大的工作, 而把自己从这种工作中解放出来, 把自己的聪明才智与创造能力贯注到更有意义的脑力劳动上去.

还应该指出, 目前我们所能证明的定理, 局限于已经发现的机械化方法的范围, 例如初等几何与初等微分几何之内. 而如何超出与扩大这些机械化的范围, 则是今后需要长期探索的理论性工作.

4. 历史的启示与中国古代数学

我们发现几何定理证明的机械化方法是在 1976 至 1977 年之间. 约在两年之后, 我们发现早在 1899 年出版的希尔伯特的经典名著《几何基础》中, 就有着一条真正的正面的机械化定理: 初等几何中只涉及从属与平行关系的

定理证明可以机械化. 当然, 原来的叙述并不是以机械化的语言来表达的, 也许就连希尔伯特本人也并没有对这一定理的机械化意义有明确的认识, 自然更不见得有其他人提到过这一定理的机械化内容. 希尔伯特是以公理化的典范而著称于世的, 但我认为, 该书更重要之处, 是在于提供了一条从公理化出发, 通过代数化以到达机械化的道路. 自然, 处于希尔伯特以及其后数学的一张纸一支笔的手工作业时代里, 公理化的思想与方法得到足够的重视与充分的发展, 而机械化的方向与意义受到数学家的忽视是完全可以理解的. 但在电子计算机已日益普及, 因而繁琐而重复的计算已成为不足道的现代, 机械化的思想应比公理化思想受到更大重视, 似乎是合乎实际的.

其次应该着重指出, 我们在从事机械化定理证明工作获得成果之前, 对塔斯基的已有工作并无接触, 更没有想到希尔伯特的《几何基础》会与机械化有任何关系. 我们是在中国古代数学的启发之下提出问题并想出解决办法来的.

说起来道理也很简单: 中国的古代数学基本上是一种机械化的数学. 四则运算与开方的机械化算法由来已久. 汉初完成的《九章算术》中, 对开平、立方与解线性联立方程组的机械化过程, 都有详细说明. 宋代更发展到高次代数方程求数值解的机械化算法.

总之各个数学领域都有定理证明的问题, 并不限于初等几何或微分几何. 这种定理证明肇始于古希腊的欧几里得传统, 现已成为近代纯粹数学或核心数学的主流. 与之相异, 中国的古代学者重视的是各种问题特别是来自实际要求的具体问题的解决. 各种问题的已知数据与要求的数据之间, 很自然地往往以多项式方程的形式出现. 因之, 多项式方程的求解问题, 也就自然成为中国古代数学家研究的中心问题. 从秦汉以来, 所研究的方程由简到繁, 不断有所前进, 有所创新. 到宋元时期, 更出现了一个思想与方法的飞跃: 天元术的创立.

"天元术"到元代朱世杰时又发展成四元术, 所引入的天元、地元、人元、物元实际上相当于近代的未知元或未知数. 将这些未知元作为通常的已知数那样加减乘除, 就可得到与近代多项式与有理函数相当的概念与相应的表达形式与运算法则. 一些几何性质与关系很容易转化成这种多项式或有理函数的形式及其关系. 这使得过去依题意列方程这种无法可循需要高度技巧的工作从此变得轻而易举. 朱世杰 1303 年的《四元玉鉴》又给出了解任意多至四个未知元的多项式方程组的方法. 这里限于 4 个未知元只是由于所使用的计

算工具（算筹和算板）的限制. 实质上他解方程的思想路线与方法完全可以适用于任意多的未知元.

不问可知，在当时的具体条件下，朱世杰的方法有许多缺陷. 首先，当时还没有复数的概念，因之朱世杰往往限于求出（正）实值. 这无可厚非，甚至在 17 世纪笛卡儿的时代也还往往如此. 但此外朱世杰在方法上也未臻完善. 尽管如此，朱世杰的思想路线与方法步骤是完全正确的，我们在上世纪 70 年代之末，遵循朱世杰的思想与方法的基本实质，采用美国数学家里特(Ritt) 在 1932, 1950 年关于微分方程代数研究书中所提供的某些技术，得出了解任意复多项式方程组的一般算法，并给出了全部复数解的具体表达形式. 此后又得出了实系数时求实解的方法，为重要的优化问题提供了一个具体的方法.

由于多种问题往往自然导致多项式方程组的求解，因而我们解方程的一般方法可被应用于形形色色的问题. 这些问题可以来自数学自身，也可以来自其他自然科学或工程技术. 在本丛书的第一本，吴文俊的《数学机械化》一书中，可以看到这些应用的实例. 工程技术方面的应用，在本丛书中有高小山的《几何自动作图与智能 CAD》与陈发来和冯玉瑜等的《代数曲面造型》两本专著. 上述解多项式方程组的一般方法已推广至微分方程的情形. 许多应用以及相应论著正在酝酿之中.

5. 未来的技术革命与时代的使命

宋元时代天元术与四元术的创造，把许多问题特别是几何问题转化成代数方程与方程组的求解问题. 这一方法用于几何可称为几何的代数化. 12 世纪的刘益将新法与“古法”比较，称“省功数倍”. 这可以说是减轻脑力劳动使数学走上机械化道路的一项伟大的成就.

与天元术的创造相伴，宋元时代的数学又引进了相当于现代多项式的概念，建立了多项式的运算法则和消元法的有关代数工具，使几何代数化的方法得到了有系统的发展，俱见于宋元时代幸以保存至今的杨辉、李冶、朱世杰的许多著作之中. 几何的代数化是解析几何的前身，这些创造使我国古代数学达到了又一个高峰. 可以说，当时我国已到达了解析几何与微积分的大门，具备了创立这些数学关键领域的条件，但是各种原因使我们数学的雄伟步伐就在这些大门之前停顿下来. 几百年的停顿，使我们这个古代的数学大国在近代变成了数学上的纯粹入超国家. 然而，我国古代机械化与代数化的光辉思想和伟大成就是无法磨灭的. 本人关于数学机械化的研究工作，就是在这些思想与成

就启发之下的产物，它是我国自《九章算术》以迄宋元时期数学的直接继承.

恩格斯曾经指出，枪炮的出现消除了体力上的差别，使中世纪的骑士阶级从此销声匿迹，为欧洲从封建时代进入到资本主义时代准备了条件. 近年有些计算机科学家指出，个人用计算机的出现，其冲击作用可与枪炮的出现相比. 枪炮使人们在体力上难分强弱，而个人用计算机将使人们在智力上难分聪明愚鲁. 又有人对数学的未来提出看法，认为计算机的出现，将使数学现在一张纸一支笔的方法，在历史的长河中，无异于石器时代的手工方法. 今天的数学家们，不得不面对计算机的挑战，但是，也不必妄自菲薄. 大量繁复的事情交给计算机去做了，人脑将仍然从事富有创造性的劳动.

我国在体力劳动的机械化革命中曾经掉队，以致造成现在的落后状态. 在当前新的一场脑力劳动的机械化革命中，我们不能重蹈覆辙. 数学是一种典型的脑力劳动，它的机械化有着许多其他类型脑力劳动所不及的有利条件. 它的发扬与实现对我国的数学家是一种时代的使命. 我国古代数学的光辉，都鼓舞着我们为实现数学的机械化，在某种意义上也可以说是真正的现代化而勇往直前.

吴文俊

2002 年 6 月于北京



前　　言

本书作者 1977 年以来，围绕被作者命名为数学机械化的这一中心，陆续发表了一系列论著，本书实质上是这些论著的一个综合报告. 所谓数学机械化，其思想实质在于以构造性与算法化的方式从事数学研究，使数学的推理过程机械化以至自动化，以尽量减少聪明才智的要求，并由此减轻艰难的重脑力劳动.

使数学机械化甚至使一切推理都自动化的愿望至少可追溯到 G. W. Leibniz(+1646, +1716). 但是，作者认为，数学机械化或更一般的推理自动化，其真正的缔造者应该是 D.Hilbert(+1862, +1943). Hilbert 关于有限基定理的存在性证明以及数学的公理化曾取得了极大成功. Hilbert 又与当时的数学权威 L.Kronecker(+1823, +1891) 曾有激烈论争，而后者可以认为是当时构造性数学的旗手. 因而 Hilbert 在数学机械化方面的功绩被长期掩盖不张. 尽管如此， Hilbert 应被认为是数学机械化的真正缔造者，这应可从他在其他众多影响巨大的成就中得到印证. 现举数例说明如下：

例 1. 1900 年巴黎的世界数学家大会上， Hilbert 作了关于数学问题的著名演讲，所列举的 23 个问题中，第 10 个问题是问如何找到解不定方程的自动化算法. 1970 年时，苏联 21 岁的青年数学家 Y. Matijasevic 给出了算法不可能存在的否定解答. 尽管如此，有关的研究却给出了对现代纯粹数学极为重要的正面结果. 参阅 M. Davis 等在 Proc. Symp in Pure Mathematics 卷 28, 1976 年的综合报告.

例 2. 1899 年 Hilbert 刊行了他的经典著作《几何基础》一书，其中有一段晦涩难明的章节. 在以后的多次再版中，这一段改写称定理 62. 经过适当注释，可以把这一章节解读为某种特殊类型几何定理的机械化或自动化证明. 其后 1950 年波兰数学家 A. Tarski 的工作以及后人在几何定理机械化证明的许多尝试，都可视为 Hilbert 在上述初等几何的一个狭隘范围的工作的延伸. 由于这一理由，作者曾把 Hilbert 书中的定理 62 重述为 Hilbert 机械化定理.

例 3. Hilbert 关于数学相容性的宏伟意愿蕴含了用一个普通的方法以自动证明数学中一切定理的庞大计划. Gödel 的发现粉碎了 Hilbert 这一过于雄心勃勃的意愿. 虽然如此， Hilbert 的努力催生了一门新的数学学科——数理逻辑，并指出了一个新的途径：不管是定理求证还是问题求解，不是一个一个地证明或一个一个地解决，而是一类一类地证明或一类一类地解决，这种处理

方式在数理逻辑学界称为定理类或问题类的可判定性. 上述 Hilbert 机械化定理, 可视为可判定性的实例, 虽简单却意义深刻而值得令人深思.

除以上数例以外, 还可提到 Hilbert 的不少论文, 其中的定理往往是以构造性与算法化的方式来证明的, 举例来说, 现在关于理想的通称为 Hilbert 函数的证明就是如此. 我们还可以注意到 Hilbert 关于有限基定理的证明, 是在于求得一有限基, 而这一有限基, 也是以构造性与算法化的方式来求得的. 本书可视为遵循 Hilbert 的思想路线, 描述数学机械化理论与方法的一个初步尝试.

全书分成三个部分, 第一部分考虑数学机械化的历史发展, 特别强调在古代中国的发展情况. 这是理所应当的. 事实上, 纯粹数学的近代发展, 大体上依照了古希腊欧几里得公理化体系这一模式. 与之相反, 中国的古代数学则是高度构造性、算法性与计算性的. 很大一部分的结果, 往往以算法的形式表达. 即使在几何这一领域, 古代中国的数学, 也对几何定理及其证明不屑一顾, 而专注于几何问题与各种问题的求解. 由此自然导致多项式方程的求解. 正因如此, 多项式方程的求解问题, 在古代中国数学中占据着中心的位置, 贯穿于几千年的发展过程. 本书遵循我国古算的这一传统, 把重点集中于多项式方程的求解, 而以几何的定理求证与几何的问题求解作为它的两个主要的应用. 这个处理的方式从本书的节题可以清楚看出.

本书的第二部分, 标题是原理与方法, 分成第三、四、五章. 这一部分的目的, 在于说明解多项式方程所依据的基本原理. 这里的方程将局限于系数所在数域的特征为零. 依据所说的基本原理, 我们将指出如何发现求解任意上述多项式方程组的一般方法. 为了这一目的, 我们将放弃通常使用的理想这一概念, 而采取多项式组零点集这一朴素而又自然的概念. 通过对多项式组零点集的分析, 在基本原理的指引之下, 引导至特征集这一概念以及有关的种种原理与定理, 如整序原理, 零点分解定理与簇分解定理等. 这些原理与定理, 构成了解任意多项式方程组方法的依据. 应该指出, 我们解多项式方程组的基本原理来源于古代的中国数学, 特别是元代 1303 年时朱世杰的《四元玉鉴》这一著作. 不言而喻, 在朱的著作中有许多疏漏而不完全之处, 但他指出了解任意多项式组的正确途径. 为了弥补朱的创作中的缺陷, 我们借助了 J.F. Ritt 关于微分方程代数研究的两本经典著作. Ritt 的工作是高度构造性、算法化与计算性的. 它们奠基于 Van der Waerden 在代数几何的早期工作. Van der Waerden 的这些早期工作与以后代数几何的现代发展不同, 基本是构造性、算法性的,

而且大体上也是计算性的. 它奠基于极为有用的母点与特定化这些概念, 而这些概念已在后来的发展中消失无踪, 对此作者深表遗憾.

作为 Van der Waerden 早期方法的一个具体应用, 在本书的 §5.3 中, 我们指出如何通过母点这一概念, 对具有任意奇点的代数簇, 也可以定义所谓陈(省身) 类与陈 (省身) 数. 虽然陈类与陈数有种种不同的推广概念, 但我们的处理方法有着独到之处. 它们是易于计算的. 举例来说, 著名的 Miyaoka - 丘不等式, 经过简易的计算, 即可推广到有任意奇点的代数簇. 而且经过计算, 中科院数学机械化研究中心的石赫还得到了一大批高维情形陈数间的不等式与等式的关系. Miyaoka - 丘不等式只是在二维无奇点曲面的一个最简单的极端情形. 以上俱见 §5.3. 关于母点概念的另一应用, 可见第三部分中的 §8.4. 这些实例说明在近代代数几何发展中已被淘汰的 Van der Waerden 早期方法的威力. 作者希望不久能给出这一早期方法的另外一些应用. 通常解多项式方程组是在复域中进行的. 但是, 当方程系数为实数时, 在实域中求解有着特别重要的意义. 一个实例是优化问题的需要, 这只有实值的解答才有意义. 在第三章中给出了一个一般的方法, 可以至少在理论上给出多项式组在复域中的全部解答. 但在实解情形, 只能取得部分成功, 答案离要求很远. 在 §5.5 中, 我们将指出, 对于有重要意义的优化问题, 可以确定一实数的有限集, 只要所求的全局最大或最小值已知存在, 则这一有限实数集的最大或最小值也就是所求优化问题的全局最大或最小值. 注意通常计算数学中用极限逼近所求得的是个别的局部的极大或极小值. 最近有实例证明, 国外文献中某些双重优化问题, 用计算数学方法加上曲折的特殊技巧, 求得所谓的全局最优化值, 其实并不是真正的全局优化值. 用我们的方法所求得的才是真正的全局最优值.

我们的全局优化方法还可以对牵涉到不等式的问题取得某些成功, 但还远不足以满意. 总之, 在实域中求解多项式组的问题, 还须进一步认真研究.

本书的第三部分的标题为应用与举例, 分成第六、七、八章. 第六章有关解多项式方程组的应用. 注意虽然本书第二部分已经说明了解系数属于零特征域的任意多项式方程组的原理与方法, 并指出至少在理论上可给出它们的全部解答, 但是这种方法有着极高的计算复杂度, 由于是符号计算, 在计算过程中往往会出现极其庞大的多项式, 使计算难以进行到底. 看来唯一的出路在于寻找某种混合算法, 融合符号计算与数值计算于一体, 使两者优势互补. 在 §6.2 中, 我们提出了这样的一种混合算法. 这一算法有着牢固的理论基础. 作者相信, 在实际中产生的多种多样的多项式方程组求解问题, 通过这一混合算

法，应大体上都可获得解决. 但我们还缺少实践，还需要真正的实例来证明这一点. 第三部分的第七章讨论几何定理的机械化证明，它将作为解多项式方程组的一般原理与方法的一个具体应用来处理. 第三部分的第八章则讨论形形色色的问题，它们表面上看来与多项式方程组不相干，但却可以通过某种方法引导至解适当的多项式方程组，然后用我们的一般方法来处理.

作为数学机械化的初步起步，本书对方程的求解全部局限于多项式的情形. 对于在几何定理证明与几何问题求解上的应用，也只是限于初等几何即不牵涉到微分运算的那部分几何学. 但在 §8.5 中，我们将约略提出把本书的理论与方法推广至微分几何与微分方程的可能发展，对于数学机械化在微分情形以及在数学其他领域中的研究，我们将俟诸异日.

作者在此对科学技术部 (前身为国家科委), 国家自然科学基金委员会，以及中国科学院表示诚挚的谢意. 没有他们在精神上的鼓励与组织上的支持，以及经济与设备方面的资助，数学机械化的研究是无法进行的，更不用说能像今天那样在国内如此繁荣了. 相信今后数学机械化的发展，还将一如既往，获得多方面的支持. 作者对在数学机械化道路上多年来志同道合共同奋斗的许多好友，特别是对于中国科学院数学与系统科学研究院数学机械化研究中心的许多同甘苦共患难的同事们致以最真挚的感谢. 由于人数众多，而且其中很大一部分都已散见于本书的各个章节，他们的姓名在此就不再一一列举了.

吴文俊

2002 年 5 月于北京

目　　录

第一部分　历史发展

第一章　古代 (中国) 多项式方程组求解 1
§1.1　中国历史和中国古代数学典籍简述 1
§1.2　中国古代解多项式方程的方法 8
§1.3　古代外国的多项式方程解法和笛卡儿方案 19
第二章　几何定理证明的历史发展和古代的几何问题求解 26
§2.1　几何定理证明，从欧几里得到希尔伯特 26
§2.2　计算机时代的几何定理证明 38
§2.3　古代中国的几何问题求解和几何定理证明 41

第二部分　原理与方法

第三章　作为零点集的代数簇和特征集方法 56
§3.1　仿射空间和投影空间的扩张点和特定化 56
§3.2　代数簇和零点集 64
§3.3　多项式集、升列和偏序 74
§3.4　多项式集的特征列和整序原理 82
§3.5　零点分解定理 93
§3.6　簇分解定理 106
第四章　计算机代数的若干问题 118
§4.1　整数组 118
§4.2　多项式理想的良序基 124
§4.3　一个多项式理想的良性基 130
§4.4　良性基的性质及其与 Gröbner 基的关系 138
§4.5　任意扩域上的多元多项式的因式分解和最大公因式 147
第五章　计算代数几何中的一些问题 158
§5.1　实代数簇与复代数簇的一些重要特征 158
§5.2　代数对应和周形式 171
§5.3　具有任意奇性的不可约代数簇的陈类与陈数 181
§5.4　拟代数簇的投影定理 189
§5.5　实多项式的极值性 197

第三部分　应用实例

第六章　在多项式方程组求解中的应用 210

§6.1 多项式方程组求解的基本原理：特征集方法 210
§6.2 一种多项式方程组求解的混合方法 218
§6.3 求解计数几何中的问题 230
§6.4 星体运动与涡流运动的中心构型 239
§6.5 机器人学中逆运动方程的求解 251
第七章　在几何定理证明中的应用 263
§7.1 几何定理机器证明的基本原理 263
§7.2 Hilbert 型几何定理的机器证明 272
§7.3 只涉及等式的几何定理机器证明 287
§7.4 涉及不等式的几何定理机器证明 297
第八章　在其他方面的应用 312
§8.1 在自动发现未知关系和自动确定几何轨迹方面的应用 312
§8.2 在不等式、优化问题和非线性规划等问题方面的应用 323
§8.3 四连杆机构设计方面的应用 333
§8.4 在计算机辅助几何设计的曲面拼接问题中的应用 340
§8.5 一些补充和扩展 349
参考文献 369

第一部分　历史发展

第一章　古代 (中国) 多项式方程组求解

§1.1　中国历史和中国古代数学典籍简述

解方程与证明定理

数学活动主要有两种，即证明定理和解方程．证明定理主要起源于古希腊，特别是起源于所谓的欧几里得几何学，而解方程则是古代中国数学的重要内容．为了说明中国古代的解方程方法，我们首先给出中国历史朝代年表．

中国历史年代简表

公元前 21 世纪，中国建立了夏朝，由散布于广阔土地上的多部落社会转变为松散的中央集权王朝．公元前 221 年，秦始皇统一中国，建立了大一统的帝国．此后，中国就从统一到分裂，又从分裂到统一，分分统统直到 20 世纪初封建王朝制度的崩溃．现将中国古代的主要朝代列表如下，公元前和公元后的年代分别用负数和正数表示．

夏 (大约 −21 世纪，−16 世纪).

殷或商 (大约 −16 世纪，−11 世纪).

西周 (大约 −11 世纪，−771).

春秋时期 (−770, −476).

战国时期 (−475, −221).

秦 (−221, −207).

西汉 (−206, +8).

东汉 (+25, +220).

三国时期 (+220, +265).

西晋 (+265, +316).

东晋和十六国 (+317, +420).

南北朝 (+420, +589).

隋 (+581, +618).

唐 (+618, +907).

五代十国时期 (+907, +960).

北宋 (+960, +1127) 和辽 (+938, +1125).

南宋 (+1127, +1274) 和金 (+1127, +1234).

元 (+1271, +1368).

明 (+1368, +1644).

清 (+1644, +1911).

<u>中国古代数学的若干特点</u>

1. 古代中国人在算板或类似器具上通过操作算筹来进行所有的计算，而不是用纸和笔计算. 1971 和 1975 年，出土了骨制和竹制的算筹，这些算筹的时代可以追溯到公元前 1 世纪或公元前 2 世纪的西汉. 见图 1.1 中的照片.

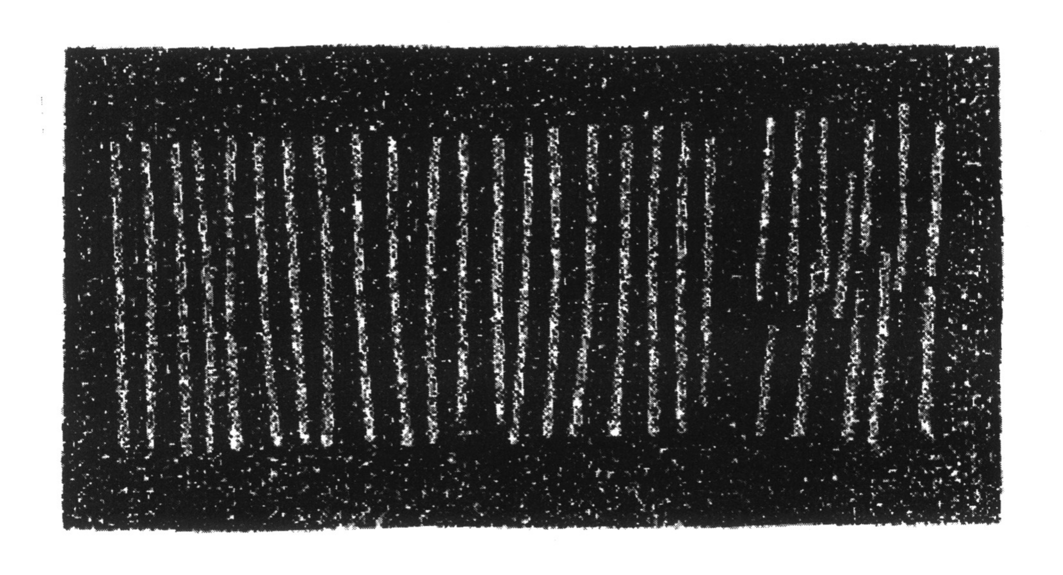


图 1.1　骨制和竹制的算筹

2. 中国人很早就掌握了极其完美的十进位值制系统，因而能够用适当地排列在算板上的算筹来表示整数. 特别地，数字 0, 不论是在整数的末尾还是在中间，都可以通过在适当的位置上留下空位来表示. 例如，整数 22022 在计算板上用筹表示为

$$|| = \quad = ||$$

在先秦时期，高效的算术运算就已得到了很好的发展. 实际上，“ arithmetic ”

这个词作为“mathematics”一词的习惯用语正是汉语“算术”的直译，意为“计数方法”.

3. (数学研究的) 最终结果通常以个别问题的形式表现出来的，每个问题都分成下列诸项内容：

(1) 以具体数据陈述的问题.

(2) 问题的数值答案.

(3) “术”，即获得答案的方法. 它常常就是我们今天所称的“算法”，有时也相当于公式或定理. 值得注意的是，(1) 中的数值在具有普遍性的“术”中并不扮演任何角色，所以可用其他同类型的任何数值来替代它. 因而，(1) 仅仅是充当一个实例，用来表明同类问题都可用这个“术”来解决.

(4) 有时有“注”，或者说是对 (3) 中方法的解释性论证. 当“术”是公式或定理时，“注”实际上就是“证明”.

(5) “草”，包含了获得最终结果的详细运算过程. 它最早出现在唐朝的一些典籍里，后来算草在宋元时期的著作中被广泛使用. 这可能是因为印刷术迅速发展的缘故.

4. 我们的祖先重视解决来自现实生活或有实际需要的问题，这些问题自然地导致方程的求解. 因此，中国古代数学，不像古希腊数学那样专注于证明定理，而是以解方程为主题. 实际上，解方程可以看作是贯穿于全部中国古代数学的一条主线，这一点将在下一节里做进一步的说明.

5. 至于几何，中国人不是去发展一套证明定理的演绎体系，而是侧重于以某种不同的证明过程为基础解决测量与几何问题. 我们将在 §2.3 中对此给予较详细的论述.

6. 总而言之，中国古代数学的特点是高度的算法化和机械化. 中国古代数学似乎是按照自己的道路发展的，它独立于可追溯到古希腊的西方数学. 可以把它看作一个机械化系统，与源于希腊并统治着现代纯数学的公理化系统迥然不同.

<u>中国古代数学典籍</u>

许多被古代文献引用过的重要数学著作都已不幸失传，其中包括由南北朝杰出的数学家、天文学家和工程师祖冲之 (+429, +500) 撰写的极其重要的《缀术》. 尽管如此，幸存下来的著作已足能反映出古代数学的概貌，并能清楚地表明中国数学的思想脉络和发展线索. 下面列举一些与我们的主题 (即解多项式方程与几何定理证明) 有紧密联系的著作.

[ZB] 《周髀算经》，大约公元前 1 世纪以前. 下文简称为《周髀》. 它是中国古代数学文献中流传到现在的最古老的典籍之一，作者不可考. 研究者认为此书的成书不晚于公元前 100 年. 与其说它是一部数学著作毋宁说它是一部天文学著作. 汉字 "髀" 意指称为表的一种天文测量工具，类似天文测量中使用的带有刻度的表杆. "周" 是秦始皇统一中国前的朝代名. 7 到 10 世纪，该书被列为国子监数学教育的十本教科书中的第一部. 尽管此书具有天文学特点，但它却包含了古代几何的重要内容，对几何的进一步发展产生了极其重要的影响. 在 §2.3 中对此将有详细叙述.

[NC] 《九章算术》，完成于公元前 2 世纪到公元前 3 世纪，下文简称为《九章》. 这是一部关于中国传统数学的综合性著作，它对中国传统数学随后的发展的影响不比欧几里得对西方数学的影响逊色. 在 1000 多年里它一直是主要的数学教科书. 在西方知识传入之前，中国的一些邻国也把它用作教科书. 与今日不同，这部著作并非由一个或几个作者完成，它更像是几代有才智的学者、知识分子、掌管天文、财政以及建筑等事务的官员们的数学成果的汇集. 该书中的许多结果和方法在秦之前很长时间就已经被广泛使用. 刘徽《九章算术注》的序言认为此书在秦之前就已经出现，但在秦朝的统治下受到了破坏. 此书经秦和西汉的高级官员张苍 (约 $-250, -152$) 和耿寿昌 (活跃于 -57 前后) 的增删，才形成了刘徽见到的样式. 几年前，在湖北的一座古墓中出土了一千多件竹简，上面刻着一本关于计算和记数的书，实际上，它是《九章》的前驱. 这些出土文物为刘徽的前言提供了明确的证据. 因此，可以保险地说，这部书的完成时间是在张苍去世之前.

[Liu1] 《九章算术注释》，+263, 刘徽. 这部著作极其重要，下文简称为 "刘徽注". 《九章》及其刘徽注是中国古代数学的代表作，可与古希腊欧几里得《几何原本》相媲美. 刘徽注为中国古代传统数学理论的发展打下了坚实的基础，还包含了大量创造性的思想以及刘徽自己的成果，对中国数学的进一步发展产生了深远的影响.

[LCF1] 《九章算术注释》，约 +656, 唐朝李淳风. 李淳风是唐朝的一位天文学家，古代数学家对他评价很高. 虽然他的注释从数学角度来看没有太大价值，但是，他在注释中加入了祖冲之之子祖暅的工作，即利用相当于后来的卡瓦列里原理来确定球体积的方法. 详见 §2.3. 必须注意的是，刘徽和李淳风的《注释》都不是独立于《九章》之外的，后来三者被整合成同一部书并在注释中明确标示，说明哪一部分注释是谁加上的.

[Liu2] 《海岛算经》，公元 3 世纪，刘徽．它本是附于《九章》之后的，后来分离出来，成为一部独立的著作．这部书的主题是用勾股工具解决测量问题．后面引用此书时，简称为《海岛》．

[ZS1] “日高图说”，公元 3 世纪，赵爽．

[ZS2] “勾股圆方图说”，公元 3 世纪，赵爽．

[ZS1] 和 [ZS2] 都是从赵爽 (三国时期或晋朝) 的《周髀》注释中摘录下来的．尽管留存的文字和图形都已残缺不全，但是从中我们仍可以得到关于古代几何的重要结论．详见 §2.3.

[WXT] 《缉古算经》， +626, 王孝通．它是一本解三次方程的著作，更详细的内容见下一节．

经过 1000 多年的发展，到 13 世纪，中国传统数学已经形成了相当完整的体系．宋元时期，中国数学成果叠现，达到了高峰，是中国数学史上发展最快、著作最多、学术水平最高的繁荣时期．在 13 世纪后半叶的几十年里，出现了四位伟大的数学家：秦九韶、李冶、杨辉和朱世杰．人们所称的宋元数学主要以这四个人的工作为代表，下面是他们的著作．

[QJS] 《数书九章》， +1247, 秦九韶．这是一部综合性著作，包含了高次代数方程的解法和所谓的中国剩余定理．该书的几何部分有许多不足，已由李倍始 (U. Libbrecht) 在他的《 13 世纪的中国数学》一书中指出．不管怎样，此书中包含了西方数学中名为霍纳公式的重要公式．详见 §2.3.

[LY1] 《测圆海镜》， +1248, 李冶．

[LY2] 《益古演段》， +1259, 李冶．这两部著作的伟大贡献是，引入了名为“天元”的未知数概念，介绍了利用未知数从给定的问题出发逐步建立代数方程的方法，为几何的代数化铺平了道路．此方法应该看作是我国古代数学中最重要的发现之一．

[YH1] 《详解九章算法》， +1261, 杨辉．

[YH2] 《日用算法》， +1262, 杨辉．

[YH3] 《杨辉算法》， +1274, +1275, 杨辉．这些著作中包含了关于应用数学和算筹简算法的内容，筹算方法的简化为现代算盘的发明铺平了道路．这些书中还包含了从其他典籍中摘录下来的片段，这些内容对我们的主要议题解多项式方程是重要的，但原作已经失传．

[Zhu1] 《算学启蒙》， +1299, 朱世杰．这是一部具有家庭教师特点的数学著作．

[Zhu2] 《四元玉鉴》，+1303, 朱世杰. 这本书的成就除了高阶算术级数和高次有限差分方法外，还把一个未知数的天元术推广到含有四个未知数的四元术. 这本书标志着我国传统数学的顶峰. 它对现代数学方法的价值与影响在下一节将有更全面的论述.

<u>中国古代数学的若干近期研究文献</u>

中国古代数学史在近年来得到了深入的研究，硕果累累，因此，我们现在对我国古代数学的理解比以往任何时候都更加深刻了. 下面列举一些我们需要特别参考的文献.

[ACTS] 《中国古代科技成就》，中国青年出版社，北京，(1978).

英译本 *Ancient China's Technology and Science*, Foreign Language Press, Beijing, (1983).

[Chen] 陈良佐，《周髀算经》勾股定理的证明与"出入相补"原理的关系，《汉学研究》，7(1989)255—281.

[Du] 杜石然，中国古代数学名著简介，[ACTS], 50—56.

[Guo1] 郭书春，高次方程数值解法与天元术，[ACTS], 111—123.

[Guo2] 郭书春，《九章算术》中的整数勾股形研究，[KJSWJ], 54—66

[Guo3] 郭书春，《古代世界数学泰斗刘徽》，山东科技出版社，(1992).

[He] 何绍庚，割圆术与圆周率，[ACTS], 90—110.

[Hoe] John Hoe, Les Systèmes d' Equation Polynomes dans le *siyuanyu-jian*(1303), Inst. Hautes Etudes Chinoise, Paris(1977).

[KJSWJ] 《科技史文集》第 8 集，数学史专集，上海科技出版社，1982.

[Kong] 孔国平，《李冶传》，河北教育出版社，1988.

[Lam] Lam Lay Yong(蓝丽蓉), The Geometrical Basis of the Ancient Chinese Square-Root Method(中国古代开平方法的几何基础),*Isis*,61 Pt.1,No.206,1970, 92—102.

[L-S] Lam Lay Yong(蓝丽蓉)、Shen Kangshen(沈康身), Methods of Solving Linear Equations in Traditional China(中国传统线性方程的解法), *Historia Math.*, 16(1989), 107—122.

[LJM1] 李继闵，刘徽对整勾股数的研究，[KJSWJ], 51—53.

[LJM2] 李继闵，《东方数学典籍〈九章算术〉及其刘徽注研究》，陕西人民教育出版社，1990.

[LJM3] 李继闵，"商高定理"辨正，《自然科学史研究》，12(1993)29—41.

[Libb] U. Libbrecht (李倍始), *Chinese Mathematics in Thirteenth Century*(13世纪的中国数学), MIT Press, (1973).

[LKW1] 李国伟, 《周髀算经》中"商高曰, 数之法出于圆方"章之研究, 第二届科学史论坛文集, 1989, 227—234.

[LKW2] Ko-Wei Lih(李国伟), From one Gnomon to two Gnomons——a Methodological Study of the Method of Double Differences, *Proceedings of 5th Intern. Congress on History of Science in China*, 1988, San Diego.

[LKW3] Ko-Wei Lih(李国伟), A New Interpretation of the Proof of Pythagorean Theorem in *Zhou Bi Suan-Jing*, 18th Inter. Congress of History of Science, 1989, Hamburg and Munich.

[Liu] 刘洁民, 关于"阳马术注"的注记, [W-B-S-T], 244—252.

[QBZ] 钱宝琮, 《中国数学史》, 科学出版社, 北京, 1962.

[Wag] D.B. Wagner(华道安), An early Chinese Derivation of the Volume of a Pyramid: Liu Hui,Third Century A.D.(早期中国对锥体体积的推导: 刘徽, 公元 3 世纪),*Historia Math.*,6(1979), 169—188.

[W-N] Wang Ling(王玲)、J.Needham(李约瑟), Horner's Method in Chinese Mathematics; Its Origin in Root-extraction Procedures of the Han Dynasty(中国数学中的霍纳法及其在汉代开方术中的起源),*T'oung Pao*, 43(1955), 345—401.

[W-B-S-T] 吴文俊、白尚恕、沈康身与李迪 (主编), 《刘徽研究》, 陕西人民教育出版社及九章出版社, 1993.

[WWT1] 吴文俊, 我国古代测望之学重差理论评介 —— 兼评数学史研究中某些方法问题, [KJSWJ], 10—30.

[WWT2] 吴文俊, 《海岛算经》古证探源, [WWT5], 162—180, 或 [WWT6], 54—73.

[WWT3] 吴文俊, 出入相补原理, [ACTS], 66—89. 或 [WWT5], 58—75.

[WWT4] 吴文俊, Recent Studies of the History of Chinese Mathematics(近年来中国数学史研究的进展), *Proc. Inter. Cong. Math.*, 1986, 1657—1667.

[WWT5] 吴文俊主编, 《〈九章算术〉与刘徽》, 北京师范大学出版社, 1982.

[WWT6] 吴文俊, 《吴文俊文集》, 山东教育出版社, 1986.

[WWT7] 吴文俊, 《吴文俊论数学机械化》, 山东教育出版社, 1996.

[Yan] 严敦杰, 中国使用数码字的历史, [KJWJ], 31—50.

§1.2　中国古代解多项式方程的方法

A. 解线性方程组与负数概念

《九章》之一例

《九章》卷 8 之标题为“方程”，内容是解线性方程组. 这一卷共包含 18 个问题，兹录第一题原文于下:

问题 1　今有上禾三秉，中禾二秉，下禾一秉，实三十九斗；上禾二秉，中禾三秉，下禾一秉，实三十四斗；上禾一秉，中禾二秉，下禾三秉，实二十六斗. 问：上、中、下禾实一秉各几何？

答曰：上禾一秉九斗四分斗之一，中禾一秉四斗四分斗之一，下禾一秉二斗四分斗之三.

方程术曰:

(1) 置上禾三秉，中禾二秉，下禾一秉，实三十九斗，于右方. 中、左禾列如右方.

(2) 以右行上禾遍乘中行.

(3) 而以直除.

(4) 又乘其次.

(5) 亦以直除.

(6) 然以中行中禾不尽者遍乘左行.

(7) 而以直除.

(8) 左方下禾不尽者，上为法，下为实. 实即下禾之实.

(9) 求中禾，以法乘中行下实，而除下禾之实.

(10) 余如中禾秉数而一，即中禾之实.

(11) 求上禾，亦以法乘右下实，而除下禾、中禾之实.

(12) 余如上禾秉数而一，即上禾之实.

(13) 实皆如法，各得一斗.

注意：上文中标号 (1),$\cdots$,(13) 系笔者所加，以说明运算步骤.

用方程术解上例的详细步骤

古代的著作通常都以非常简明的形式写成，逐字地研究上面的句子有时是困难的. 然而，(1)~(13) 的运算步骤对说明其确切含义已经足够清晰了.

步骤 (1) 将题中数据按下列方式在筹算板上排成三列:

$$\left[\begin{array}{c|c|c} 1 & 2 & 3 \\ 2 & 3 & 2 \\ 3 & 1 & 1 \\ 26 & 34 & 39 \end{array}\right]$$

接下来的步骤包括了如下形式的一系列推导:

$$\xrightarrow[(2)]{}\left[\begin{array}{c|c|c} 1 & 6 & 3 \\ 2 & 9 & 2 \\ 3 & 3 & 1 \\ 26 & 102 & 39 \end{array}\right] \xrightarrow[(3)]{}\left[\begin{array}{c|c|c} 1 & 0 & 3 \\ 2 & 5 & 2 \\ 3 & 1 & 1 \\ 26 & 24 & 39 \end{array}\right]$$

$$\xrightarrow[(4)]{}\left[\begin{array}{c|c|c} 3 & 0 & 3 \\ 6 & 5 & 2 \\ 9 & 1 & 1 \\ 78 & 24 & 39 \end{array}\right] \xrightarrow[(5)]{}\left[\begin{array}{c|c|c} 0 & 0 & 3 \\ 4 & 5 & 2 \\ 8 & 1 & 1 \\ 39 & 24 & 39 \end{array}\right]$$

$$\xrightarrow[(6)]{}\left[\begin{array}{c|c|c} 0 & 0 & 3 \\ 20 & 5 & 2 \\ 40 & 1 & 1 \\ 195 & 24 & 39 \end{array}\right] \xrightarrow[(7)]{}\left[\begin{array}{c|c|c} 0 & 0 & 3 \\ 0 & 5 & 2 \\ 36 & 1 & 1 \\ 99 & 24 & 39 \end{array}\right]$$

$$\xrightarrow[(9)]{}\left[\begin{array}{c|c|c} 0 & 0 & 3 \\ 0 & 180 & 2 \\ 36 & 0 & 1 \\ 99 & 765 & 39 \end{array}\right] \xrightarrow[(11)]{}\left[\begin{array}{c|c|c} 0 & 0 & 540 \\ 0 & 180 & 0 \\ 36 & 0 & 0 \\ 99 & 765 & 4995 \end{array}\right]$$

步骤 (8), (10) 和 (12)(以及 (13) 的总结) 分别给出: 下禾一秉: 二斗四分斗之三; 中禾一秉: 四斗四分斗之一; 上禾一秉: 九斗四分斗之一.

<u>《九章》中负数的引进</u>

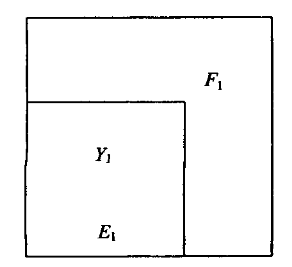
在现在汉语数学词汇中,"方"和"程"两个汉字放在一起意味着 equation(方程). 实际上, 汉字"方"现在意为正方形, 然而在古代它还有一些其他的含义. 根据刘徽注, 汉字"程"指把数据排成若干列. 从上面的例子可以看出, 不管古代的原始含义是什么, "方程"应该解释为"方阵", 而"方程术"正是以某些确定的方法对这样的方阵进行操作, 最后达到某些标准形式, 以便获得最

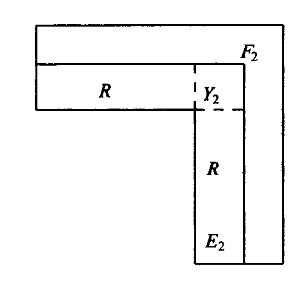
终的答案．相应的“术”描述的程序具有相当普遍的特点．不过，在相减的步骤中可能发生一些 (正) 数减掉更大的数的情况．事实上这种情况发生在该章第 3 题中．正是在这里引进了正数和负数的概念．据刘徽注，这两种数是用红色和黑色两种不同颜色的算筹来加以区分的．《九章》的“正负术”给出这些数的加减规则．除此之外，第 2 题中涉及数据转换的运算，支配这种运算的规则由下面的术给出：“损之曰益，益之曰损．”上面的 3 个术，实际上构成了现代意义上解线性方程组方法的核心．《九章》卷 8 的成就无疑是遥远的古代一系列发展的结果．《九章》卷 2 、3 和 6 中各种比例问题的解法以及卷 7 中的盈不足术似乎是卷 8 一般方法的先导．但是，这些发展的轨迹仍不清楚．

B. 二、三次方程的解法与 13 世纪高次代数方程的数值解法

九章中的开平方术

最简单的二次方程是形式为 $x^2 = A$ 的方程，其中 A 是大于 0 的整数，这个方程相当于求 A 的平方根．在古代中国，开平方根这类问题来源于土地面积的测量，自然还来源于勾股研究，即：给定勾股形的两边，确定另一边．前者及相关问题是《九章》卷 4 的主题，后者及相关问题是卷 9 的内容．卷 4 第 12~16 题是已知方田面积求边长的问题．这样的问题是由被称为 开方术 的算法来解决的，后来中国所有的求高次代数方程正根的方法实质上都是由此术扩展而来．实际上，在中国古代数学典籍中的开方与我们今天所谓的解方程是同意的．由于开平方法的重要性，我们应该对相应算法的细节作深入研究．为此，以卷 4 第 12 题为例．这个问题是：已知正方形的面积为 55225 个单位，确定其边长．这个算法说明了边长的确定是如何一步一步进行下去的．但是要看出解题过程中隐含的规则却很困难．正是刘徽的注释清楚地说明了隐含在其中的以几何为基础的规则，并且附加了一个图解，图中的各个区域用不同颜色标示．尽管这一图解已经失传了，但是根据注释，很容易将它重新复原出来，大致如图 1.2.





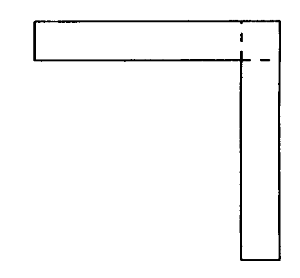


图 1.2　《九章》中的开平方术

在图 1.2 中，Y 和 R 部分分别对应着原图的黄色和红色，下标 1 和 2 则对应于古代中国历法中表顺序的天干名. 确定 55225 平方根的方法如下.

方田 F 的面积为 55225. 很早以前中国就已经拥有了完善的整数十进位值制系统. 因此，首先确定所求边长是一个三位数即最高位在百位上. 因为 $2^2 < 5 < 3^2$, 估得给定面积将包含一个边长为 $2*10^2$ 的较小的正方形 Y_1, 姑且称这个估得的边长数值为正方形 Y_1 的“法”, 并用 E_1 表示. 现在, 从给定的正方形中减去正方形 Y_1, 则剩下一个面积为 $55225-(2*10^2)^2=15225$ 的磬折形 F_1. 区域 F_1 的内边长已知为： $2*$法 $=4*10^2$, 称其为“定法”. 为了得到区域 F_1 的宽，首先确定这个宽度是一个二位数. 因为 $3*4<15<4*4$, 可以确定，磬折形区域 F_1 将包含一个相同形状的区域 (即图 1.2 中的 $R+R+Y_2$). 其宽度的估值为 $E_2=3*10$. 这个区域的面积显然为： 定法$*E_2+E_2^2=400*30+30^2=12900$. 去掉这个区域我们得到了一个面积为 $15225-12900=2325$ 的更小的磬折形区域 F_2. 区域 F_2 的内边长为： 定法 $+2*E_2=4*10^2+2*3*10=460$, 仍称为“定法”或“定法$_2$”. 按照上面的程序进行下去，我们得到下一个数位将在个位上，该位上的估值是 5. 这表明，在去掉一个宽度为 $5*1$ 的更小的磬折形后区域 F_2 将被穷尽. 这样就得出给定区域 F 的边长为 $2*10^2+3*10+5=235$.

面或无理数的概念

开方术算法无非是上述程序的算术化，而上述程序是以颇具一般性的几何思考为基础的. 此外，卷 4 中也给出了不一定是整数的分数开方法. 然而，至为重要的是紧随其后的一句话：“若开之不尽者，为不可开，当以面命之.”刘徽注中，对这句话的解释也极其重要，刘徽说：

术或有以借算加定法而命分者，虽粗相近，不可用也. 凡开积为方，方之自乘当还复其积分. 令不加借算而命分，则常微少，其加借算而命分，则又微多. 其数不可得而定. 故惟以面命之，为不失耳.

刘徽把这与分数的引进相对比. 当限制在整数范围内除法不能进行时，就引入分数. 刘徽以 10 除以 3 为例来解释，因为在整数范围内不能除尽，所以迫使人们引进一个作为实体的分数 1/3. 类似地，当不可开方时，开之不尽的方根被定义为“面”. “面”与现代意义的无理数是等价的. 这个概念在《九章》原文中就已经被明确地引进和解释了. 而刘徽的注释在很长一段时间里被中国数学史家们忽略了，直到 1992 年才被西安西北大学的李继闵确切指出，见其书 [LJM2]. 李继闵进一步指出，在《九章》及其刘注中有与“面”或无理数

相关的结果，这些结果相当于等式：

$$(\sqrt{N})^3=\sqrt{N^3},\quad N=\sqrt{N^2},\quad \sqrt{M}*\sqrt{N}=\sqrt{M*N},$$

$$\sqrt{\frac{M}{N}}=\frac{\sqrt{M}}{\sqrt{N}},\ \sqrt{\frac{M}{N}}=\frac{\sqrt{M*N}}{N},\ \sqrt[3]{\frac{M}{N}}=\frac{\sqrt[3]{M}}{\sqrt[3]{N}},\ \sqrt[3]{\frac{M}{N}}=\frac{\sqrt[3]{M*N^2}}{N}.$$

注意，最后四个等式是以分数开方为基础的，在《九章》原文中已经出现.

<u>分数开方与完整的十进位值制系统</u>

除了引进“面”这个相当于无理数的重要概念外，刘徽对开方还提出了一些同样重要的建议. 实际上，基于我们自古以来就已使用的完美的整数十进位值制，刘徽建议，把开方程序进一步进行下去，从而确定与 $\frac{1}{10},\frac{1}{10^2},\cdots$ 相对应的相继各位数字. 刘徽说：

退之弥下，其分弥细，则朱幂虽有所弃之数，不足言之也.

因此，刘徽所建议的实际上是采用完善的十进位值制来任意精确地逼近任何实数. 但不幸的是，这个重要的建议被中国的学者们忽略了几个世纪. 不管怎样，至少在 10 个世纪之后，这个系统最终被采纳并应用到代数方程数值解的逼近中. 至于在欧洲，我们清楚地知道，斯蒂文 (Stevin, +1548, +1620) 于 1585 年在他的《论十进》中引进了十进分数，并被看作一项重大成就而备受赞扬.

<u>带从开方</u>

重新回到开方术，我们看到在开方过程中会遇到这样的情况：设磬折形 F 是由一个已知面积为 A 的正方形在一角上去掉一个边长为 a 的小正方形而得. 这样 F 就具有已知面积： $A-a^2=B$. 这个程序表明，我们能够解决下面的问题：

问题 Q 已知面积为 B 内边为 $2*a$ 的磬折形区域 F, 求区域 F 的宽 x.

让我们考虑由图 1.2 得来的图 1.3, 这里令 $E_1=a$, F_1 的未知边长则用 x 来表示. 这样我们就看到面积等于 $B=A-a^2$ 的区域 F 是由两个红色的子区域 R 和一个黄色的子区域 Y 构成的，每一个 R 的面积为 $a*x$, Y 的面积为 x^2. 这样用现代符号我们有

$$x^2+2*a*x=B\quad(a>0,B>0)\tag{1.2.1}$$

或

$$(x+a)^2-a^2=B\quad(a>0,B>0).\tag{1.2.2}$$

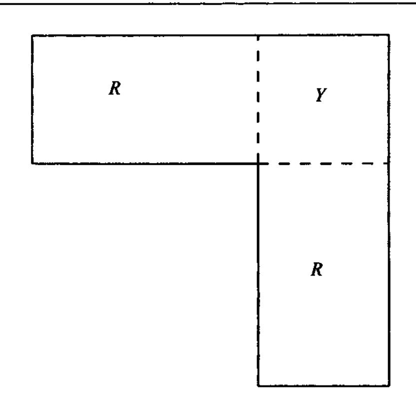


图 1.3 磬折形 F

现在把两个红色子区域中的一个移到黄色区域的一侧得到一个图 1.4 所示的矩形区域. 那么这个矩形的面积与磬折形 F 的面积是一样的. 这个矩形区域

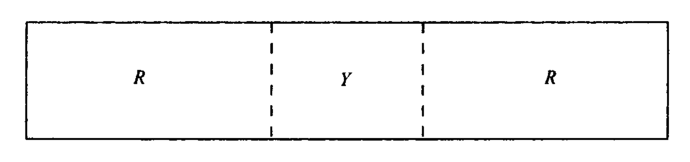


图 1.4 矩形区域

的两边的差为 $2*a$, 等于磬折形区域的内边, 在开方过程中称为定法. 这样, 开方术的程序也可以解决如下的问题:

问题 $\boldsymbol{R}$ 给定面积为 B, 两边之差为 $2*a$ 的矩形, 确定矩形的短边.

我们的祖先称问题 Q, R 或相当于解二次方程 (1.2.1), (1.2.2) 的问题为"带从开方". 这里 从 或 从法 是一个与磬折形 F 的内边相对应的值 $2*a$, 它在开方术过程中称为"定法", (1.2.1) 中的 B 在古书中称为"实", 意为面积, 实即磬折形 F 或相应矩形的面积.

<u>带从开方例题</u>

我们再取《九章》卷 9 的"邑方问题"作为例子.

第 20 题 今有邑, 方不知大小, 各中开门. 出北门二十步有木. 出南门一十四步, 折而西行一千七百七十五步, 见木. 问: 邑方几何?

答曰: 二百五十步.

术曰: 以出北门步数乘西行步数, 倍之为实. 并出南门步数为从法. 开方除之, 即邑方.

注意这里"步"是古代长度单位 (1 步 = 5 尺; 3 尺 = 1 米). 分别用 n, s 和

w 表示向北、向南和向西的步数. 上术说明, 第 20 题可以当作问题 R 来解决, 其中实或矩形的面积为 $B=2*n*w=71000$, 从或两边之差为 $2a=n+s=34$. 用现代符号表示相当于解下面的方程:

$$\left.\begin{array}{l} x^2+(n+s)*x=2*n*w, \\ x^2+34*x=71000. \end{array}\right\} \tag{1.2.3}$$

在 §2.3, 我们将据刘徽注解释原来的第 20 题是怎样转变成问题 R 的. 参见图 1.5 和 1.6.

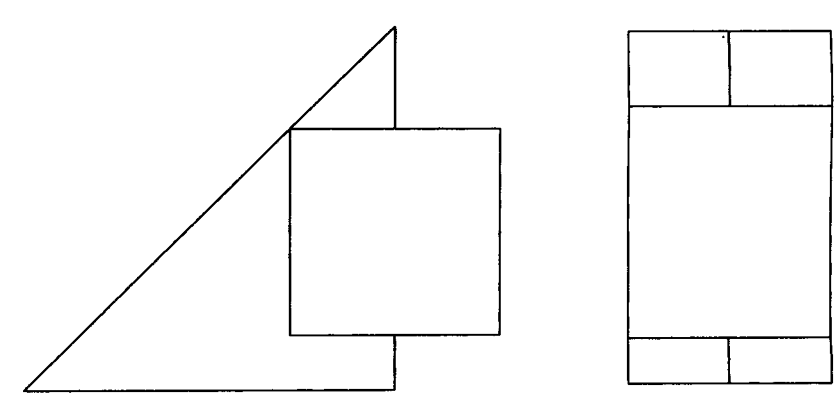


图 1.5 《九章》中的第 20 题

图 1.6 问题 R

《九章》中的开立方术

在《九章》卷 4 中还有 *开立方术*, 它与下面图 1.7(此图与 1.2 是相似的) 所展示的几何程序的算术化是相对应的.

如前所述, 在开方过程中, 我们会遇到下面的情况: 从给定体积的正方体 V 的一角去掉一个边长为 a 的小正方体, 如图 1.7. 我们得到一个图 1.8 中的立体 S, 体积为 $W=V-a^3$. 开立方术的程序使我们可以确定对角上的小正方体的边长. 使用现代的符号, 我们令该边长为 x, 则从图 1.8 我们看到立体 S 由 7 个长方体构成, 边长为 a, a, x 的 3 个, 边长为 a, x, x 的 3 个, 边长为 x, x, x 的 1 个. 用现代符号, 这个程序相当于解如下形式的三次方程:

$$x^3+3*a*x^2+3*a^2*x=W \quad (a>0, W>0) \tag{1.2.4}$$

或

$$(x+a)^3-a^3=W \quad (a>0, W>0). \tag{1.2.5}$$

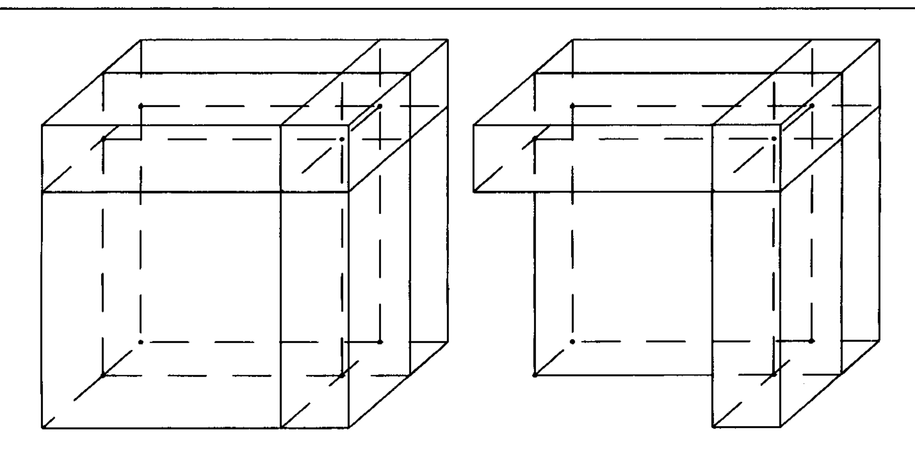


图 1.7 《九章》中的开立方术 a　　　　图 1.8 《九章》中的开立方术 b

一般评述

公元 3 世纪，赵爽在他的“勾股圆方图说” [ZS2]* 中已经给出了关于勾股形的若干命题. 一些历史学家认为，这些命题以可以解释为以明确的形式给出了二次方程. 然而，我们的祖先对于获得明确的公式来得到形如 (1.2.1), (1.2.2) 或更一般的二次方程的根似乎没有兴趣，他们更感兴趣的是获得二次方程的满足实际要求的数值解. 对于 (1.2.4), (1.2.5) 或更一般形式的三次方程也是如此.

汉朝到唐朝的三次方程

对于三国时期之后一直到祖冲之 (+429, +500) 时代的中国数学的发展，我们知之甚少. 在《隋书 · 律历志》中记载了祖冲之计算 π 值的伟大成就，还有他的”开差幂”、”开差立”. 数学史家钱宝琮把它们解释为带从开平方和立方的方法，相当于解方程

$$x*(x+k)=A \quad 或 \quad x^2+k*x=A(k,A>0)$$

和

$$x*(x+k)*(x+l)=V \quad 或 \quad x^3+(k+l)*x^2+k*l*x=V(k,l,V>0).$$

不幸的是，祖冲之的著作失传了，我们很难去确证钱宝琮的推断. 不管怎么说，祖冲之的创造被他的儿子所继续，王孝通在其著作《缉古算经》 [WXT] 中对后者的工作提出了严厉的批评. 由于没有有关的原著，我们也无从得知王孝通批评他的理由.

王孝通有关三次方程的著作

王孝通的著作《缉古算经》 [WXT] 是一部专门研究三次方程的作品，出现于公元 7 世纪的唐初. 该书包含了 20 个问题，这些问题大部分来源于大型建筑工程. 为解决这些问题，王孝通首先说明了如何建立三次方程，接着用带从开立方法得到结果. 用现代符号表示，这些方程具有形式

$$x^3 + a_1 * x^2 + a_2 * x = a_3 \quad (a_1, a_2, a_3 > 0). \tag{1.2.6}$$

在每一个例子中，王孝通都根据给定的数据给出求 a_1, a_2, a_3 的算式，这些算式非常复杂，但他未给出其推导过程. 一旦 a_i 确定了，王孝通就简单地说，“开 (带从) 立方除之, 即某某”. 对当时的学者们来说, 大概求三次方程 (1.2.6) 的数值解的方法是众所周知的，因此王孝通没有必要作更多的解释.

宋朝高次代数方程的数值解

王孝通的著作之后一直到北宋 (+960, +1038), 这方面的进展不大. 后来取得的突破归功于贾宪，他的主要著作似乎出现在 +1023~+1050 这段时间. 这些著作都已失传. 万幸的是，在后来杨辉 (生活于南宋末期) 的著作 [YH1, 2, 3] 中，贾宪的方法和大量的问题被重新提及. 根据杨辉的著作，我们获知，贾宪的方法就是一种高次开方法，或相当于解

$$x^n = A \quad (A > 0) \tag{1.2.7}$$

形式的方程，其中 n 是大于 3 的正整数. 解方程 (1.2.1), (1.2.2), (1.2.4), (1.2.5) 的开平方术和开立方术都是以几何思考的算术化 (如图 1.2,1.3,1.7,1.8 所示) 为基础的，但是，对于更高次的方程这样的几何考虑不再有效了. 另外，根据杨辉的著作，在贾宪时代就已经出现了所谓的“开方作法本源”图，这种图实际上与 17 世纪所谓的帕斯卡三角是一样的. 由此看来，贾宪已经使自己从几何思考中解放出来了，而且在“开方作法本源”图的帮助下，从先辈们的算术化开方术出发直接得到了他的方法. 此外，在贾宪时代，不仅能够解出方程 (1.2.7)，而且还应该能够求出如下形式的方程的数值解：

$$x^4 + 4 * a * x^3 + 6 * a^2 * x^2 + 4 * a^3 * x = D \quad (a > 0, D > 0) \tag{1.2.8}$$

或

$$(x + a)^4 - a^4 = D \quad (a > 0, D > 0). \tag{1.2.9}$$

对贾宪方法的进一步改进是由刘益在其已失传的著作《议古根源》中作出的 (12 世纪). 幸运的是，刘益著作中的方法和许多问题在杨辉的著作中也被提

及. 在幸存下来的问题中有一个是解方程

$$-5*x^4+52*x^3+128*x^2=4096. \tag{1.2.10}$$

因此, 刘益已经摆脱了方程的系数必须为正 (像 (1.2.8) 那样) 这一限制. 在秦九韶的《数书九章》 [QJS] 中, 贾宪和刘益的方法已经被融合在一起, 并发展成为一个普遍的方法, 称为“正负开方术”, 它可以求出次数任意高、系数可为正、为负或为零的代数方程的数值解. 正如刘徽所做的一样, 在秦九韶的方法中自由地使用了十进小数. 秦九韶的方法实际上与所谓的霍纳法 (+1819 年) 是一样的. 因此, 从《九章》中的开方术开始经过 15 个世纪不断的努力, 中国人终于达到了自己的目标: 可求出任意次数、任意数值系数的代数方程的数值解.

C. 宋元时期的天元术与解多元方程的消元法

天元术与几何代数化

宋元时期最重要的发明就是被称之为“天元”的明确的未知数概念的引入. 宋元数学家发展了所谓的“天元术”, 这个方法可以方便地把几何量转变为多项式形式, 把几何关系转变为多项式方程. 这时出现了李冶 (+1192, +1279) 的两部著作《测圆海镜》 [LY1] 和《益古演段》 [LY2], 并流传至今. 第一部完成于 +1248 年, 专门研究应用天元术的一些问题. 第二部写于 +1259 年, 其目的是普及天元术. 天元术可以简要概述为: 先设某个未知数为天元, 然后将其他量以两种不同的方式用未知数天元的多项式表达出来, 然后通过使它们相等得到一个方程, 而这个方程可以用当时已经发展得很好的方法求解. 最后求解的方程可能具有相当高的次数, 在《测圆海镜》 [LY1] 的 170 个题目中, 出现了 13 个 3 次、 13 个 4 次和 1 个 6 次方程. 应注意的是, 尽管从《九章》时代起解方程就已经得到了很好的发展, 但当时还没有明确的未知数概念, 因而, 建立方程是一件非常困难的工作, 它常常以复杂的几何思考为基础. 天元概念的引进使这样的工作变得非常容易完成. 清朝的学者张敦仁应用天元术轻而易举地建立起王孝通在《缉古算经》 [WXT] 中用特别繁琐的步骤才找到的那些三次方程. 此外, 李冶在他的著作中还引进了相当于今天多项式及其运算的概念, 开辟了通向几何代数化的道路. 还应注意的是, 秦九韶的著作《数书九章》 [QJS] 与李冶的《测圆海镜》 [LY1] 几乎是在同时完成的, 但是他们都未提到对方的任何著作. 看起来他们彼此之间根本就不认识. 实际上秦九韶生活在中国的南部而李冶生活在中国的北部, 当时南北两地分别属于战争中两

个敌对王朝的统治之下. 这两位学者的研究旨趣也不一样, 一位对已经建立起来的方程的数值解感兴趣, 另一位则把主要精力放在建立方程上. 他们的工作互为补充, 交相辉映. 二者合在一起, 正是中国古代数学黄金时期的标志.

<u>高次多项式方程的解法与消元方法</u>

早在《九章》中就已经有了多元线性方程组的求解方法, 宋元时期则出现了解只有一个未知数的高次多项式方程的方法. 那么, 把这两种方法统一起来, 用于解不限于单个未知数的高次多项式方程组, 就非常自然了, 而且事实也确是如此. 在李冶的著作中就已经出现了这样的问题, 如果引进多个而非一个未知数就更易于建立起方程来. 但是李冶本人并未能做到这一点, 他一直只使用一个未知数. 对于后来的学者来说, 把这个方法拓展到多于一个未知数的好处应该是明显的. 实际上, 我们知道, 曾有过这样的著作, 讲述通过天、地二元两个未知数建立两个方程的方程组和有三个未知数、三个方程的方程组的方法, 但这些书籍都失传了. 幸运的是, 元朝朱世杰的《四元玉鉴》(+1303年)[Zhu2] 幸存了下来. 这本书处理的多项式方程甚至达到了四个未知数 (分别称为天、地、人, 物), 所用方法是一种顺序消元法. 它是以一些消元程序为基础的, 其过程大致如下. 首先指定未知数为天等等, 并建立方程. 假设有四个这样的含四个未知数的方程. 选择其中的一个未知数从给定的方程组中消去它, 得到一个有三个未知数的三元方程组. 接着从这个三元方程组中进一步消去一个未知数, 得到一个二元方程组. 最后, 从这两个方程中消去两个未知数中的一个, 得到一个只有一个未知数的方程. 再用已知的方法解这个方程, 然后把所得到的解代入到其他方程中, 顺序求解便得到各个未知数的值. 这显然是一种普遍方法, 它特别依赖于多项式的演算及消元法. 因此, 某种代数和几何的代数化也就应运而生.

<u>朱世杰的一个例子</u>

通过《四元玉鉴》 [Zhu2] 中的典型例子可以清晰地了解朱世杰的方法. 下面是其中一例: 由一个几何问题导出一个含有三个未知量的三元方程组, 以现代记号可以写成如下形式:

$$\left.\begin{aligned} &x*y*z-x*y^2-z-x-y=0,\\ &x*z-x^2-z-y+x=0,\\ &z^2-x^2-y^2=0. \end{aligned}\right\} \tag{1.2.11}$$

欲解出 z. 朱世杰的方法大略如下: 因为几何量 x 不能为 0, 所以 x 在下面的过程中可以自由地作除数. 首先在 (1.2.11) 中消去 y, 得到二元方程组, 接着逐

步降低所得方程组中 x 的次数，最后将得到只含有 x 和 z 的两个方程，并且这两个方程对 x 来说都是线性的．再从这两个方程中消去 x，得到一个只含有 z 的方程，即

$$z^4 - 6 * z^3 + 4 * z^2 + 6 * z - 5 = 0. \tag{1.2.12}$$

朱世杰选择这个方程的正数解 $z = 5$ 作为所求解．关于上述运算的详细介绍可以在优秀的论文 [Hoe] 中找到．

对朱世杰方法的评论

朱世杰在解上题时，求得 $z = 5$ 就停止了．然而，我们可以再往下做一步，取只含 x 和 z 并且关于 x 是线性的两个方程中的任一个，及 (1.2.11) 中的任一个 (比如说第二个) 方程，与方程 (1.2.12) 一起组成一个三元方程组

$$\left.\begin{aligned} &z^4 - 6 * z^3 + 4 * z^2 + 6 * z - 5 = 0, \\ &x * (7 + 3 * z - z^2) - (6 + 7 * z + 3 * z^2 - z^3) = 0, \\ &y - (x * z - x^2 - z + x) = 0. \end{aligned}\right\} \tag{1.2.13}$$

则我们可以顺次解出 (1.2.13) 的未知数 z, x 和 y, 得到三元解 (z, x, y)．如果从 $z = 5$ 开始，将得到解 $(5, 3, 4)$．方程 (1.2.12) 除了 $z = 5$ 外还有另外两个解 $z = -1, +1$．若取 $z = -1$, 可得到三元解 $(z, x, y) = (-1, 1, 0)$, 可以验证这个解是原方程组 (1.2.11) 的解．如果取 $z = 1$, 则三元解 $(z, x, y) = \left(1, \frac{5}{3}, -\frac{4}{9}\right)$，它不是原方程组 (1.2.11) 的解．

在朱世杰时代，为了实际的计算，必须把多项式各项的系数以算筹的形式摆放在算板的确定位置上．这样这个方法就受到了限制，只能处理最多含有四个未知数的四个方程，而且只有较简单的方程才能这样求解．然而，有一点是清楚的，即朱世杰的方法具有普遍性，它能够被应用于任意方程组．另一方面，对上述特例的分析表明，这个方法同时也存在着很大的缺陷，需要加以完善．本书的主要目的之一就是对这个由朱世杰发展起来的数学方法给出一个坚实的数学基础，这件事将在第三章中完成．明朝以来，中国古代数学在算法方面的辉煌发展开始走下坡路了，对世界数学不复产生影响．

§1.3 古代外国的多项式方程解法和笛卡儿方案

国外的数学史出版物

在西方有关数学史的出版物浩如烟海，这些文献偶尔涉及日本、印度或阿拉伯的数学史，但是关于中国数学史的却凤毛麟角．下面列举一些我们需要参

考的出版物.

[AA] A. Aaboe, *Episodes from the Early History of Mathematics* (《早期数学史片断》), Yale University, 1964.

[Caj] F. Cajori, *A History of Mathematics* (《数学史》), 第二版, Macmillan,1919.

[Des1] R. Descartes, *La Géomètrie*(《几何学》), Leiden, 1637.

[Des2] R. Descartes, *Rules for the Direction of Mind* (《指导思维的准则》), 英译本, 载 E. S. Haldane & G. R. T. Ross, *The Philosophical Works of Descartes* (《笛卡儿的哲学著作》), Cambridge University Press, 1911.

[Ev] H. Evens, *An Introduction to the History of Mathematics* (《数学史概论》), 第五版, Saunders Colledge Publishing, 1983.

[Kar] L.C. Karpinski, *Robert of Chester's Latin Translation of the Algebra of al-Khwarizmi* (《花拉子米〈代数学〉: Robert of Chester 的拉丁文译本》), New York,1915

[Kl] M. Kline, *Mathematics Thought from Ancient to Modern Times* (《古今数学思想》), Oxford University Press, 1972.

[LWL1] 李文林, 笛卡儿《几何学》的机械化特征, 《自然科学史研究》, 12(1993), 225—234.

[LWL2] 李文林, 算法、演绎倾向与数学史分期, 自然辩证法通讯, Vol.8, No.2, 1986, 46—50.

[M] Y. Mikami (三上义夫), *The Development of Mathematics in China and Japan* (《中国与日本数学的发展》), 第二版, Chelsea, 1974.

[N] J. Needham, *Science and Civilization in China* (《中国的科学与文明》), Vol.3, Cambridge University Press, 1959.

[P] G. Polya, *Mathematical Discovery*(《数学发现》), Vol.1, John Wiley & Sons, 1962.

[Sc] J. F. Scott, *A History of Mathematics from Antiquity to the Beginning of the Nineteenth Century* (《从古代到 19 世纪初的数学史》), Dover Publ., 1958.

[Sm] D. E. Smith, *History of Mathematics* (《数学史》), Vol.1, Vol.2, Dover Publ., 1958.

[S-L] D. E. Smith & L. M. Latham, *The Geometry of Renè Descartes* (《笛卡儿的几何学》), Dover Publ., 1954.

[St] D. J. Struik, *A Concise History of Mathematics* (《数学简史》), Dover Publ. 1948, 1967, 1987.

[VdW] B. L. Van der Waerden, *A History of Algebra, from al-Khwarizmi to Emmy Noether* (《代数学史：从花拉子米到艾米 · 诺特》), Springer, 1985.

<u>线性方程组</u>

在古代，除了中国之外，并未听说有线性方程组解法. 至于线性方程组的消元法，通常把它归功于高斯，名为高斯消元法. 这个方法第一次出现在高斯的论文 [Gau3] 中.

<u>二次方程</u>

在公元前 3 世纪欧几里得的《几何原本》中，有与几何作图相关的命题，即著名的关于黄金比率的命题 11 和命题 28, 29. 若用现代的形式解释，它们相当于解某些二次方程. 波斯人花拉子米 (约 +813, +850) 的著作《代数学》(*Hisab Al-jabr W'al Muqabala*)(+830) 首先详细地研究了线性方程和二次方程的解法. 这些二次方程被分成了 5 种类型，用现代符号可以表示为

$$a*x^2=b*x,\quad a*x^2=b,\quad a*x^2+c=b*x,$$

$$a*x^2+b*x=c,\quad a*x^2=b*x+c.$$

其中 a, b, c 都是正数. 花拉子米的解法具有几何特征，和中国古代应用出入相补原理对几何体进行划分的方法极其相似，参见 2.3 节. 花拉子米的书名表明，我们今天的某些术语可能是来自于 *al-jabr* 这个词. 另一方面，史密斯认为，*al-jabr* 的基本意思是负量的转移，而 *muqabala* 是正量的转移和同类项化简. 参见 [Sm], 卷 2, 第 389 页.

<u>花拉子米工作的来源</u>

在 [VdW] (p.13) 中，范德瓦尔登 (Van der Waerden) 讨论了花拉子米的工作特别是其代数学的来源. 他说："这方面已经有三种理论被提出来：他可能使用了古希腊的文献；或者印度的文献；或者属于希腊和后希腊传统的通俗数学作品."

上述三个来源中的最后一个，范德瓦尔登似乎指的是叙利亚 - 波斯传统包括希伯莱传统的东西. 在 [N] (p.107, 147) 中，李约瑟认为古代中国的数学很可能是花拉子米工作的另一个来源. 李约瑟写道：

人们有理由问：阿拉伯数学难道未曾受到中国人在这方面的影响？从这一点出发研究花拉子米的原著将是有益的. 他曾经于 +842 年到 +847 年作为大使被哈里发派往哈扎王国，而哈扎王国正好横跨在中国到西方的商道上.

关于哈扎王国，李约瑟在关于以色列和哈扎王国的附录 ([N], pp.681~683) 中进一步写道：

……哈扎国是知道中国人的，而且可汗使用中国的官廷礼仪. ……作为哈扎王国可能在科技交流中扮演角色的一个例子，我们想起了 +842 年至 +847 在那里当大使的伟大的代数学家花拉子米.

除了上面所提出的花拉子米工作可能的来源之外，笔者倾向于认为花拉子米的工作是其自己的创造. 实际上颇有一些数学史家，如斯特洛伊克，在其著作 [St] 中认为，早在公元前 3 世纪的巴比伦时期，人们就已经知道怎样解二次甚至更高次的方程和联立方程组，甚至还知道怎样用二次方程的系数表示根. 如果这是真的，就没有理由不相信经过 1000 多年之后，在几乎与巴比伦相同的土地上会有一些数学天才作出像花拉子米的工作那样的创造.

三次和高次方程

在阿拉伯世界，阿布尔 · 瓦法 (Abu'l-Wafa) 给出了一些特殊二次方程的几何解. 后来奥马海亚姆 (Omar Khayyam, 约 +1044, +1123) 给出了三次方程的系统分类，并通过考虑圆与二次曲线图形的交点给出了三次方程的几何解. 在欧洲，费罗 (Scipione del Ferro, +1465, +1526) 在 1515 年前后研究了三次和二次方程. 这类研究继续开展，直到卡尔丹 (Cardano, +1501, +1576) 和费拉里 (Ferrari, +1522, +1565) 发现了三次和四次方程的解法. 卡尔丹的具有几何特征的三次方程解法标志着欧洲数学在黑暗的中世纪沉寂了几百年后开始上升. 与古代中国人主要致力于代数方程的数值解以满足实际需要的做法不同，欧洲的数学家像卡尔丹和费拉里所做的那样，更热衷于寻找方程的用系数严格表示的根式解. 经过大约三百年的努力之后，才最终发现这样的努力注定是要失败的，这主要归功于阿贝尔 (Abel, +1802, +1829) 和伽罗瓦 (Galois, +1811, +1832) 发现了一般根式解的不可能性，他们的工作导致了伽罗瓦理论和群论等 19 世纪的重大成就. 至于代数方程的数值解法则是由霍纳 (W. H. Horner, +1786, +1837) 在 1819 年得到的，这个方法现在以他的名字命名. 正如伊夫斯在《数学史概论》 [Ev] (p.159) 中引述的那样，霍纳完全没有意识到这个事实：他只不过重新发现了古代中国人的算法.

负数

克莱因在《古今数学思想》 [Kl] 中指出 (p.185)：

印度人引进负数代表债务；在这种情况下，正数代表财产. 现知第一个使用 (负数) 的是婆罗摩笈多 (约在 628 年)，他还叙述了负数的四则运算法则. 婆

什迦罗则指出正数的平方根有两个，一正一负.

由此可知，至迟在婆罗摩芨多时代 (约 628 年), 印度人就很好地知道了负数的性质极其运算. 至于西方世界的情况，我们可以引述克莱因 [Kl] (p.252) 的如下论述:

至于负数，尽管欧洲人已经通过阿拉伯的书籍逐渐知道了它，但十六七世纪的大多数数学家并不接受它. 即使接受，也不把它看作方程的根.

克莱因在 [Kl] (p.593) 中进一步说:

实际上，即使在笛卡儿 1637 年的《几何学》中，代数方程的负根还被指称为“假根”.

必须注意的是，古代中国人也是只接受代数方程的正根，但情形有所不同. 因为古代中国人考虑的主要是来自于实际的问题，只有正根才使他们感兴趣. 另一方面，他们很清楚地知道负数的含义，并把负数和正数混合起来自由地进行运算. 这一点我们在前面讲述《九章》卷 8 中的题目时已经看到了.

笛卡儿的问题解决方案

波利亚在他的经典著作《数学发现》 [P] 的第 2 章把我们的注意力引向了笛卡儿的遗作 [Des2]. 波利亚描述了笛卡儿的一个期望适用于所有类型问题的概要性方案. 现转述如下:

首先，把任一问题转化为数学问题.

第二，将任一数学问题转变为代数问题.

第三，将任一代数问题转变为单个方程求解.

第三步可以进一步解释. 根据波利亚的论述，我们知道:

笛卡儿建议我们建立与未知数个数一样多的方程，令 n 代表未知数的个数， $x_1, x_2, \cdots, x_n$ 代表未知数本身；这样我们可以把所求的方程组写成如下的形式:

$$
\begin{gathered}
r_1(x_1, x_2, \cdots, x_n) = 0, \\
r_2(x_1, x_2, \cdots, x_n) = 0, \\
\cdots\cdots \\
r_n(x_1, x_2, \cdots, x_n) = 0,
\end{gathered}
$$

其中 $r_1(x_1, x_2, \cdots, x_n)$ 代表 $x_1, x_2, \cdots, x_n$ 的多项式，其他方程的左边也做相同的解释. 笛卡儿建议进一步把这个方程组化成为一个最终的方程.

对“笛卡儿方案”的若干评述

在提出把一切问题转化为多项式方程求解方面，笛卡儿看起来是有些异

想天开. 在笛卡儿时代微积分尚未建立, 他自然不知道微分方程以及除多项式方程以外的其他方程. 但是, 即使一个问题能够如此地转化为多项式方程, 方程的个数与未知数的个数也可能不一致, 可能多也可能少. 即使方程数与未知数个数相同, 对于如何把这样一个多项式方程组化简成只有一个未知数的方程, 人们还是不甚了了, 并且这决不是一件轻而易举的事. 即使能够做到这种化简, 也可能产生多余的解或丢掉解. 正像波利亚在上述著作中指出的一样, 化简后的含有一个未知数的方程实际上只是在"一般的" (即在"正则的"情况下) 才能提供原方程组的全部解. 而要弄清什么是"一般的"或"正则的"的情形又谈何容易! 这一点可以从最简单的情形 (即 r_i 对诸 x 均为线性的情形) 就看出. 实际上, 澄清这方面的问题正是本书的主要目标之一, 这将在第三章中进行. 不过, 尽管笛卡儿的方案似乎显得荒谬, 我们还是要从波利亚的著作中摘录如下的段落:

笛卡儿的计划失败了, 但它仍不失为一个伟大的计划, 而且即使失败了, 它对数学的影响也超过了偶尔获得成功的千万个小计划. 尽管笛卡儿的方案不是对所有的情形都可行, 但是它确实对无穷多种情形行之有效, 其中包括无穷多种重要的情形.

事实上今天我们看到, 确实存在着无数来自于数学、科学和技术等等方面的问题, 能够被最终化为解多项式方程的问题. 在各种各样的方程组中, 具有多项式形式的那些显然是最简单的和最基本的, 但同时所解决的问题又完全是非平凡的. 因此, 在所有数学问题之中, 多项式方程的求解问题应被看作是需要优先解决的最重要的问题之一.

"笛卡儿方案"与中国古代数学

在最近的一篇论文 [LWL1] 中, 李文林分析了笛卡儿的 [Des1], 我们摘录李文林的若干观点如下:

1. 用笛卡儿的方法, 几何被算术化, 因而, 几何问题转化为解代数方程.

2. 对任一种 (代数) 方程, 都存在根的给定的一些"标准"的几何作图或者说"标准"的求解方法.

3. "标准"可以看作是某种"机械化"过程.

4. 笛卡儿的《几何学》可以看作是"笛卡儿方案"在几何领域经过补充和改进之后的实现. 实际上, 从 [Des1] 来看, 笛卡儿显然具有这样的态度: 强调通过解方程来解决几何问题, 而不是通过证明定理来求解几何问题, 这与我们祖先的精神是一致的.

比较笛卡儿与我们的祖先获得这个目标的方法似乎是有意义的. 为此, 让我们引述 [Des1] (p.6) 中的一段话:

于是, 当要解决某一问题时, 我们首先假设解已经得到, 并给为了得出此解而可能要用到的所有线段指定名称, 不论它们是已知的还是未知的. 然后在对已知和未知数线段不作区别的情况下, 利用这些线段间最自然的关系, 将难点化解, 直至找到这样一种可能, 即用两种方式表示同一个量. 这将引出一个方程, 因为这两个表达式之一的各项合在一起等于另一个的各项.

在前一节中, 我们解释了我们的祖先引进天元等未知数建立方程的方法. 把笛卡儿关于建立方程的方法的这段话与我们祖先的方法做一番比较, 是十分有趣的. 总而言之, 可以说中国古代数学发展的主流与"笛卡儿方案"所体现的方向不谋而合, 反之, "笛卡儿方案"可以看作是对中国古代数学发展道路的一种理论概括.

第二章　几何定理证明的历史发展和古代的几何问题求解

§2.1　几何定理证明，从欧几里得到希尔伯特

<u>几何定理证明的发展阶段</u>

定理证明，作为一种脑力劳动，是人们在数学上最主要的工作方式之一．它起源于古希腊并以欧几里得的《几何原本》为代表作．根据历史学家的考证，该书大约于公元前 300 年问世．然而，自从欧几里得时代以来，人们对几何定理证明的认识和处理经历了若干阶段，以下将解释这一点．

阶段 I．欧几里得风格的几何定理证明

几乎每个人在中学时代就熟悉欧几里得风格的几何定理证明，这种风格的证明具有以下两个特点．

(1) 定理的证明是基于公理系统，通过逻辑推理导出，并通过定义 - 公理 - 定理 - 证明的形式表述．

(2) 每个定理有一个只为它本身所特有的证明．

<u>示例：　毕达哥拉斯定理和海伦公式</u>

几何定理证明并不存在一般的方法，它需要高度的智力和通过一种迂回曲折的方式来寻找．一个看似很简单的定理的证明往往却很难找到．为了与古代中国和后来的定理证明方式作比较，我们将从欧几里得时代以来发现的无数美妙有趣的定理中选出几个例子．

例 2.1.1 (毕达哥拉斯定理)　在直角三角形中，斜边的平方等于两直角边的平方和．

这个定理在欧几里得的《原本》中是第 47 个命题．普洛克鲁斯 (Proclus,+410 或 +412～+485) 认为，这个定理的推导完全归功于毕达哥拉斯 (大约 −560～ −480)．以下给出《原本》中关于这个定理的图形 (图 2.1．在《原本》中此前还没有出现面积这个概念，该定理中出现的等式是指某种类型的图形 “分割相等”，在后面的第二节将对该问题进行讨论．

例 2.1.2 (海伦公式)　三角形三边长分别为 a, b, c，设 $s = \dfrac{a+b+c}{2}$，则三角形面积为

$$\triangle = \sqrt{s*(s-a)*(s-b)*(s-c)}.$$

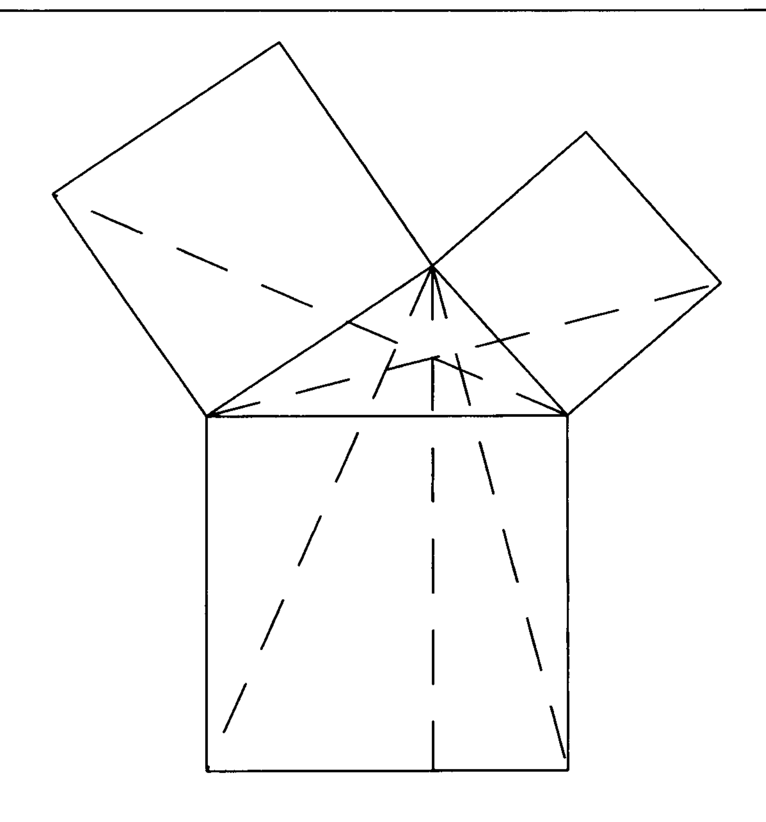


图 2.1 毕达哥拉斯定理

该公式的证明通常认为由亚历山大的海伦 (Heron), 在 +62 年左右完成. 下面我们仅根据希斯 (T.L.Heath) 所编《欧几里得原本十三册》(卷二，第 87 页), 给出与海伦证明相关的附图 (图 2.2). 该图形出现在海伦的著作《度量》(Metrica) 和《屈光学》(Dioptra) 中.

笛卡儿关于几何的经典著作

1637 年笛卡儿经典著作《几何学》(La Géomètrie) 的问世导致了几何定理证明的一种全新的方法. 在该书的法文版中，笛卡儿开宗明义的一个小标题就是:

怎样使算术运算与几何运算相联系？

笛卡儿接着在正文中说明了几何作图如何与 $a+b, a-b, a*b, a/b, \sqrt{a^2+b^2}$ 等基本算术运算相联系，其中 a,b 为线段的长度. 然后，他解释如何通过使用隐含的坐标系，将这种方法应用于各种各样的几何与光学问题. 这一创造在今天被称为解析几何，它为把几何归约为代数 (或用笛卡儿自己的术语即算术)

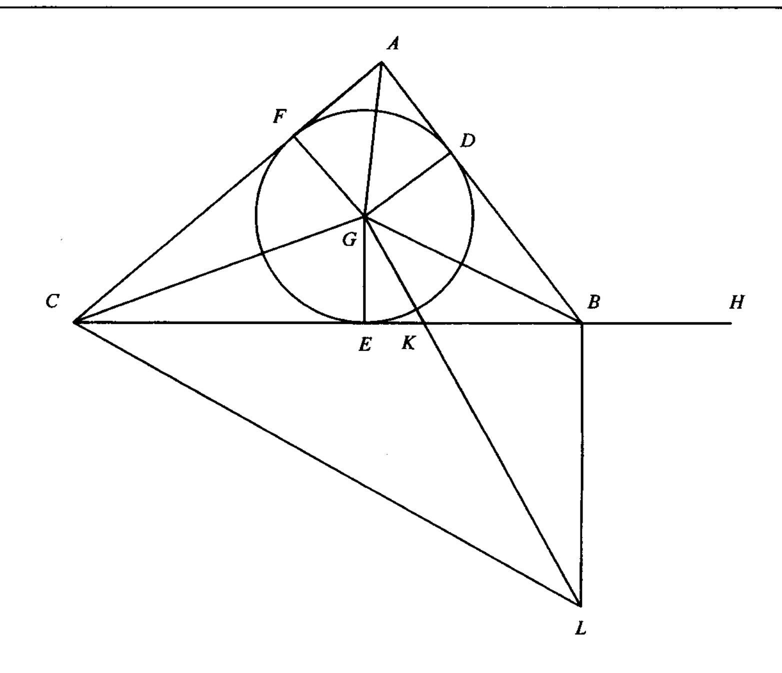


图 2.2　海伦公式

以及用纯代数运算来代替逻辑推理铺平了道路. 几何定理证明从此进入了一个崭新的阶段.

<u>示例: 高斯定理</u>

为了探讨笛卡儿的几何定理证明的风格, 我们先考虑高斯发现的一个定理.

用现代术语代替高斯当时的术语, 我们称平面上四条直线构成的一个图形为 *完全四边形*, 若这四条直线相交于六个不同的点. 如图 2.3. 其中 AEB, AFD, BCF, CDE 这四条线组成了一个完全四边形. 三对交点 $(A,C),(B,D)$, 和 (E,F) 的每一对都不同时落在这四条直线的任何一条上, 因此称它们为对角对. 高斯在一篇短文中证明了与这样一个四边形的四条直线相交的所有二次曲线的中心共线. 由于这三组对角对每一组都可以被看作一条退化的二次曲线, 且同这四条直线相交, 很容易就得出如下推论.

例 2.1.3 (高斯线定理)　对一个完全四边形, 三组对角对的中点共线.

高斯定理的欧式证明需要添加辅助线, 推理也比较复杂. 这样的证明可以在通常的几何教科书中找到, 这里我们不再讨论. 另一方面, 高斯本人似乎颇为这条定理感到自豪, 因为他认为这是一条新定理. 他写道:

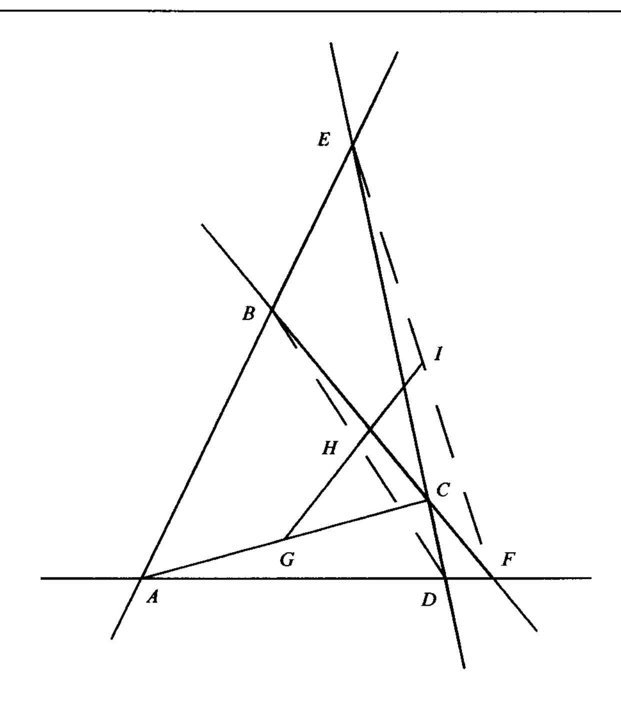


图 2.3 高斯线定理

据我所知，迄今还没有人注意到关于任意四边形的这个一般性质. 下面我就对此性质给出一个简单而直接的证明.

我们现在用高斯自己的记号复述他的证明. 我们任意取一个坐标系并设相关各点为 $A=(a,a')$, $B=(b,b')$ 等. 类似地，我们令对角对 $(A,C),(B,D)$ 和 (E,F) 的中点为 $G=(g,g'),H=(h,h')$, 和 $I=(i,i')$, 则

$$g=\frac{1}{2}*(a+c),\quad g'=\frac{1}{2}*(a'+c'),\quad \text{等等}.$$

几何条件 (A,E,B) 三点共线将转化为代数等式:

$$a*(e'-b')+b*(a'-e')+e*(b'-a')=0.$$

类似地，另外三组 $(A,F,D),(B,C,F),(C,E,D)$ 三点共线之几何条件将分别转化为代数等式:

$$a*(f'-d')+d*(a'-f')+f*(d'-a')=0,$$
$$b*(c'-f')+c*(f'-b')+f*(b'-c')=0,$$
$$c*(e'-d')+d*(c'-e')+e*(d'-c')=0.$$

把这四个等式相加，得到

$$(a+c)*(e'+f'-b'-d')+(b+d)*(a'+c'-e'-f')+(e+f)*(b'+d'-a'-c')=0,$$

这等同于

$$g*(i'-h')+h*(g'-i')+i*(h'-g')=0,$$

于是 (G,H,I) 三点共线得到证明.

笛卡儿风格的几何定理证明

从上述例子看出笛卡儿方法使得几何定理证明进入了一个新的阶段.

阶段 II. 笛卡儿风格的几何定理证明.

我们看到笛卡儿风格与第一阶段欧几里得风格的主要区别是在于其特征 (1) 被以下特征 $(1)'$ 所取代:

$(1)'$ 证明仅仅通过计算进行.

另一方面特征 (2) 没有发生变化. 对每一个定理我们都必须找到某种方法处理相关的代数方程, 而这种处理方法只适用于该定理. 而且, 找到这样的方法进行定理证明并不简单. 通过前面的高斯定理证明, 我们已经可以看到, 尽管比欧几里得风格的情形要好不少, 处理代数方程仍需要机智和技巧. 况且, 计算的工作量可能很大以致于难以控制. 这也许正是强有力的笛卡儿几何定理证明方法并没有在中学的解析几何课程中教授的原因.

希尔伯特的经典著作《几何基础》

几何定理证明风格更为彻底的变革是由 1899 年问世的希尔伯特的经典著作《几何基础》引发的. 在这本经典著作中, 希尔伯特展示了如何在欧几里得公理系统的基础上通过引入某种数系来导出笛卡儿坐标系, 如下所示:

公理系统 $\longrightarrow$ 数系 $\longrightarrow$ 坐标系统

由此, 希尔伯特在欧几里得的逻辑演绎法与笛卡儿的计算法之间架造了一座桥梁. 注意希尔伯特所说的数系相当于现代术语中的 域. 与笛卡儿的处理类似, 这样的域是由线段的运算决定的. 所不同的是它基于几何公理系统.

希尔伯特著作中的希尔伯特定理类

与欧几里得或笛卡儿的一理一证的风格不同, 希尔伯特在上述经典著作的若干章节中提出要证明一整类定理而不是一个定理. 在第一版的第 6 章第 35 节中, 有一段斜体字的论断在以后的各版中变成了定理. 我们引述如下:

定理 62 设一种平面几何中, 公理 $\mathrm{I}_{1-3}, \mathrm{II}, \mathrm{IV}^*$ 都满足, 而且巴斯嘎定理正确. 这几何中的每一条纯粹的交点定理, 可以通过作适当的辅助点和辅助直线, 表为有限个巴斯嘎构形的组合.

希尔伯特对上述定理中的"纯粹的交点定理"解释如下:

所谓一条纯粹的交点定理，所指的是具有下述性质的定理：只含有关于点和直线的位置关联以及关于直线的平行性的叙述，而同时不用其他关系 (例如，合同和垂直).

希尔伯特隐含地对这样的纯粹的交点定理加上了约束，即在这个定理中涉及到的点和线应该是按某种确定的次序逐个引入. 事实上，希尔伯特这样写到：

首先任意取一组有限个点和直线，然后按照预定的方式作这些直线中的某些任意平行线，在这些直线中的某些直线上取任意点，而且通过这些点中的某些点作任意直线；在按照预定的方式作了连线，交点以及通过已经存在的点的平行线之后，终于得到一组有限条直线，它们就是定理所论断的，通过同一个点或互相平行的直线.

我们称可以用上述方式描述的纯交点定理为 *构造性* 纯交点定理. 我们可以清楚看出：所谓构造性纯交点定理的全类，或者简称为希尔伯特定理类，包括了无数多个定理，其中有很多广为人知的定理，它们与 Pappus, Desargues, Pascal, Steiner, von Staudt 等名字联系在一起.

希尔伯特定理类中的一个例子：Desargues 定理

接下来我们引用一个属于希尔伯特定理类的例子：

例 2.1.4 (Desargues) 定理(投影形式) 对于投影平面上的两个三角形，如果对应顶点的连线共点，则这两个三角形三对相应的边的交点共线. 该定理的逆也成立.

这个定理是由投影几何的先驱 Desargues(+1593, +1662) 所发现，首先是对同一投影空间中两个不共面的三角形情形，使用欧几里得方法给出了该定理的证明，接着又推导了两三角形共面的情形.

我们将研究该定理的一种特殊情形. 希尔伯特的经典著作指出，这种情形对研究欧几里得几何基础有很重要的意义.

例 2.1.5 (Desargues) 定理(特殊形式) 对于欧几里得平面上的两个三角形，如果对应顶点的连线共点或平行，且有两对对应边平行，则第三对对应边也平行. 反之，如果两个三角形三对对应边相互平行，则这两个三角形对应顶点的连线共点或平行.

希尔伯特定理类中定理的通用证明

现在让我们来考察一下希尔伯特在数学方面惊人的贡献：尽管构造性纯交点定理的全类或希尔伯特类包含有无限多条定理，希尔伯特却指出了：所有这些定理可以用同一种通用的方法来证明. 由于希尔伯特这一观点的深远意

义，我们摘引希尔伯特的整段原文如下：

开始时我们完全任意取了点和直线，把它们的坐标看作是参数 $p_1,\cdots,p_n$；然后我们又在有限度的任意性之下取了点和直线，它们的若干坐标能够看作是另一些参数 $p_{n+1},\cdots,p_r$，其余的都将由 $p_1,\cdots,p_r$ 这些参数决定了. 以后再作出的所有的连线，交点和平行线的坐标，都是依赖于这些参数的诸有理式 $A(p_1,\cdots,p_r)$. 在这样的情形下，所要证明的交点定理的内容化为下述的论断：当参数值相同时，某一些这种的式子取相同的值；换句话说，交点定理就是说：当参数 $p_1,\cdots,p_r$ 用所讨论的几何中所引进的线段计算中的任意元素代入时，这些参数的某一些完全确定的有理式 $R(p_1,\cdots,p_r)$ 都等于零. 既然这些元素的域是无穷的，我们从一条已知道的代数定理得到下述结论：在 13 节中的运算律 1~12 的基础之上，这些式子 $R(p_1,\cdots,p_r)$恒 等于零，但是要想证明式子 $R(p_1,\cdots,p_r)$ 在我们的线段计算中恒等于零，根据我们在上文所证明了的关于应用运算律的事实，应用巴斯噶定理就足够了，这样，我们证明了下述结论：

定理 62 ···

因此，尽管定理 62 的叙述本身比较隐晦，在这个定理叙述之前的段落已经清楚地表明希尔伯特已经展示了怎样用一个通用的方法证明一整类无数多条定理.

<u>希尔伯特通用证明方法的机械化程序</u>

接下来我们用自己的方式来描述希尔伯特的通用方法 (我们写参数时用 u_i 来代替 p_i)：

希尔伯特的通用证明程序：

第一步. 取坐标系.

第二步. 相继地引入点和线.

第三步. 引入参数 $u_1,u_2,\cdots,u_r$ 并且依次引入约束变量 $x_1,x_2,\cdots,x_s$，使要证明的几何定理的假设条件依次被转化成以下形式：

$$\begin{aligned}
x_1 &= \frac{P_1(u)}{Q_1(u)},\\
x_2 &= \frac{P_2(u,x_1)}{Q_2(u,x_1)},\\
&\cdots\\
x_s &= \frac{P_s(u,x_1,\cdots,x_{s-1})}{Q_s(u,x_1,\cdots,x_{s-1})}.
\end{aligned} \tag{2.1.1}$$

在这些等式中所有的 P_i, Q_i 都为关于参数 $u=(u_1, u_2, \cdots, u_r)$ 和前述约束变量 $x_1, \cdots, x_{i-1}$ 的有理函数. 定理的结论也被转换为以下形式:

$$R(u, x_1, \cdots, x_s)=0, \tag{2.1.2}$$

这里 R 代表一个有理函数.

第四步. 通过 (2.1.1) 依次从 R 中消去 $x_s, x_{s-1}, \cdots, x_2, x_1$, 使得

$$R(u, x_1, \cdots, x_s) \longrightarrow R_1(u, x_1, \cdots, x_{s-1}) \longrightarrow \cdots \longrightarrow R_{s-1}(u, x_1) \longrightarrow R_s(u).$$

第五步. 如果 $R_s(u)=0$, 我们就可以断言定理在条件

$$Q_i(u, x_1, \cdots, x_{i-1}) \neq 0 \tag{2.1.3}$$

下成立. 否则得出该定理不成立, 至少是在条件 (2.1.3) 下不成立. 这时该定理就被认为是不成立.

示例: 用希尔伯特通用方法证明 Desargues 定理

我们注意到为了使得在上述类中的一条定理成立, 像 (2.1.3) 这样的限制是必不可少的. 下面我们将把这样的限制称为非退化条件. 为了看到它的几何意义, 我们来证明例 2.1.5 中的 Desargues 定理:

设两个三角形分别为 ABC 和 $A'B'C'$. 考虑如下情形, 即直线 AA', BB', CC' 交于同一点 O, 并且直线 AB 平行 $A'B'$, AC 平行 $A'C'$. 证明直线 $BC, B'C'$ 也平行. 见图 2.4.

我们按照上述的步骤来证明. 第一步, 选择点 O 为原点, 通过该点的任意两条直线为倾斜的 X 轴和 Y 轴. 然后, 选取 X 轴上任意的点 $A=(u_1, 0), A'=(u_2, 0)$, Y 轴上任意点 $B=(0, u_3)$, 以及平面上任意的点 $C=(u_4, u_5)$. 通过点 A' 作一条平行于 AB 的直线交 Y 轴于点 $B'=(0, x_1)$, 于是

$$x_1=\frac{u_2 * u_3}{u_1}. \tag{2.1.4}$$

连接 AC, OC 并通过点 A' 作一条直线平行于 AC 交 OC 于点 $C'=(x_2, x_3)$. 由几何条件, 即 CC' 通过原点 O 并且直线 AC 同直线 $A'C'$ 平行, 得到

$$u_4 * x_3-u_5 * x_2=0, \tag{2.1.5}$$

$$(u_4-u_1) * x_3-u_5 *(x_2-u_2)=0. \tag{2.1.6}$$

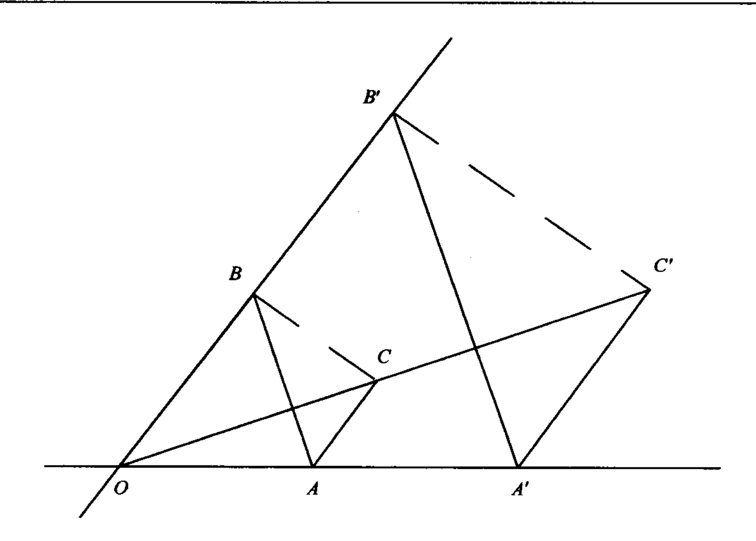


图 2.4 用希尔伯特通用方法证明 Desargues 定理

由于 u_i 为独立参数，我们特别地有

$$u_1 \neq 0, \quad u_4 \neq 0, \quad u_5 \neq 0. \tag{2.1.7}$$

在条件 (2.1.7) 下两个等式 (2.1.5),(2.1.6) 可以改写为

$$\left.\begin{aligned} x_2 &= \frac{u_2 * u_4 * u_5}{u_1 * u_5}, \\ x_3 &= \frac{u_5 * x_2}{u_4}. \end{aligned}\right\} \tag{2.1.8}$$

等式 (2.1.4),(2.1.8) 构成了该定理的假设. 结论直线 BC 和直线 $B'C'$ 平行则相当于

$$u_4 * (x_3 - x_1) - (u_5 - u_3) * x_2 = 0. \tag{2.1.9}$$

为了证明该定理，必须逐个消去等式 (2.1.9) 左边的 x_3, x_2, x_1. 计算过程为

$$\begin{aligned} & u_4 * (x_3 - x_1) - (u_5 - u_3) * x_2 \xrightarrow[(2.1.8)_2]{} u_4 * (\frac{u_5 * x_2}{u_4} - x_1) - x_2 * (u_5 - u_3) \\ = \; & -u_4 * x_1 + u_3 * x_2 \xrightarrow[(2.1.8)_1]{} -u_4 * x_1 + \frac{u_2 * u_3 * u_4 * u_5}{u_1 * u_5} \xrightarrow[(2.1.4)]{} 0. \end{aligned}$$

由此可见，如果等式 (2.1.7) 即非退化条件满足的话， Desargues 定理成立.

<u>关于希尔伯特通用方法的一些评述</u>

我们进一步考虑证明 Desargues 定理时的条件 (2.1.7). 如果 $u_1 = 0$, 将导致 A 同 O 重合，使得该定理缺乏几何意义. 如果 $u_4 = 0$, 将使点 C 位于 Y 轴上. 点 C' 将成为 Y 轴上一个确定的点. 这个情形表明在一些退化情形下该定理仍可能成立，如图 2.5. 另一方面，如果 $u_5 = 0$ 则将导致点 C 位于 X 轴上，C' 将成为 X 轴上任意一点. 这说明了在某些退化情形，假设条件仍然满足，但结论直线 BC 同直线 $B'C'$ 平行却不再成立. 参见图 2.6. 因此， (2.1.7) 中的非退化条件 $u_5 \neq 0$ 对于该定理成立是必不可少的.

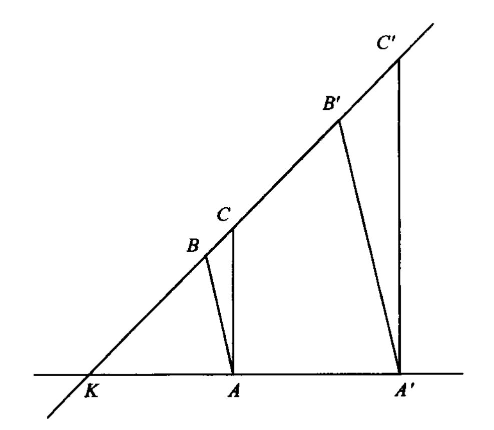


图 2.5 退化情形下该定理仍可能成立

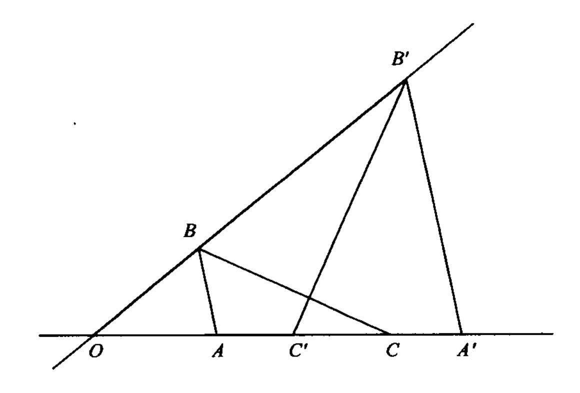


图 2.6 直线 BC 同直线 $B'C'$ 不再平行

由此可见非退化条件 (2.1.7) 对于该定理是否有意义或是否成立是必不可少的. 注意到这对于几何定理来说是一种普遍现象，我们将在第七章作进一步

讨论并给出更多的例子.

进一步的示例：高斯定理的证明

为了解释希尔伯特几何定理的通用证明方法，我们现在来重新考察例 2.1.3 中所讨论的高斯定理. 尽管该定理不属于希尔伯特类，但希尔伯特几何定理证明的通用方法对它仍然适用. 更详细的讨论请看 §2.2 或者 §7.2.

我们再参看图 2.3. 考虑通过依次逐个引进点和线一步一步地将图形画出而不是一下子画出整个图形. 这样我们将按照以下的步骤来完成这个图形.

首先，在平面上任意取一点 A 为坐标原点. 通过点 A 任意作两条直线，使其成为斜坐标系统的 X 轴和 Y 轴. 再在 Y 轴上选取任意一点 B, 令其坐标为 $(0,u_1)$, u_1 作为一个参数来显示该点的任意性. 然后在平面上任意选取一点 C 并令其坐标为 (u_2,u_3), 同时在 X 轴上任取一点 D, 使其坐标为 $(u_4,0)$. 所有的 u 都代表参数. 连接 C,D 并使其同 Y 轴交于点 E, 因为 E 的坐标不是任意的，令其为 $(0,x_1)$, 显而易见 x_1 满足

$$x_1=\frac{u_3*u_4}{u_4-u_2}. \tag{2.1.10}$$

注意在这里我们已经假设 $u_4-u_2\neq 0$, 同时也假设 DC 同 Y 轴 AB 不平行，这样 E 就被合理地定义了，同时 x_1 也能由上面的表达式确定. 现在作一条直线连接 B,C 并与 X 轴 AD 相交于点 F, 显然， F 将不是一个任意的点. 设其坐标为 $(x_2,0)$, 则 x_2 将由下式确定：

$$x_2=\frac{u_1*u_2}{u_1-u_3}. \tag{2.1.11}$$

如前面一样假设 $u_1-u_3\neq 0$ 或 BC 不平行于 X 轴. 现在对于点 A,C 我们令其中点 G 的坐标为 (x_3,x_4), 于是可得

$$x_3=\frac{1}{2}*u_2,\quad x_4=\frac{1}{2}*u_3. \tag{2.1.12}$$

分别连接 B,E 和 D,F 并设这两条直线的中点分别为 $H=(x_5,x_6)$ 和 $I=(x_7,x_8)$, 得到

$$x_5=\frac{1}{2}*u_4,\quad x_6=\frac{1}{2}*u_1, \tag{2.1.13}$$

$$x_7=\frac{1}{2}*x_2,\quad x_8=\frac{1}{2}*x_1. \tag{2.1.14}$$

等式 (2.1.10)~(2.1.14) 组成了我们所讨论的高斯线定理的假设. 这个定理的结论对应于下列方程：

$$\begin{vmatrix} x_3 & x_4 & 1 \\ x_5 & x_6 & 1 \\ x_7 & x_8 & 1 \end{vmatrix} = 0. \tag{2.1.15}$$

为了证明，我们从结论 (2.1.15) 式的左边开始，借助于假设方程 (2.1.14), $\cdots$, (2.1.11), (2.1.10) 一步步地将 $x_8, x_7, \cdots, x_2, x_1$ 消去. 全部计算过程如下：

$$\begin{vmatrix} x_3 & x_4 & 1 \\ x_5 & x_6 & 1 \\ x_7 & x_8 & 1 \end{vmatrix} \overrightarrow{(2.1.14)} \begin{vmatrix} x_3 & x_4 & 1 \\ x_5 & x_6 & 1 \\ \frac{1}{2}*x_2 & \frac{1}{2}*x_1 & 1 \end{vmatrix} \overrightarrow{(2.1.13)} \begin{vmatrix} x_3 & x_4 & 1 \\ \frac{1}{2}*u_4 & \frac{1}{2}*u_1 & 1 \\ \frac{1}{2}*x_2 & \frac{1}{2}*x_1 & 1 \end{vmatrix} \overrightarrow{(2.1.12)}$$

$$\frac{1}{4}*\begin{vmatrix} u_2 & u_3 & 1 \\ u_4 & u_1 & 1 \\ x_2 & x_1 & 1 \end{vmatrix} \overrightarrow{(2.1.11)} \frac{1}{4}*\begin{vmatrix} u_2 & u_3 & 1 \\ u_4 & u_1 & 1 \\ \frac{u_1*u_2}{u_1-u_3} & x_1 & 1 \end{vmatrix} \overrightarrow{(2.1.10)} \frac{1}{4}*\begin{vmatrix} u_2 & u_3 & 1 \\ u_4 & u_1 & 1 \\ \frac{u_1*u_2}{u_1-u_3} & \frac{u_3*u_4}{u_4-u_2} & 1 \end{vmatrix}.$$

前面已经指出等式 (2.1.10) 和 (2.1.11) 的分母不为零，有了这个条件很容易证明最终的表达式等于零，也就是证明了高斯线定理是成立的.

同前面的按照欧几里得风格和笛卡儿风格的证明相比较可以看出，个人的机智和技巧在这里的定理证明中所起的作用甚微，甚至于一个只懂得初等几何知识的外行也可以不太费劲地完成这样的定理证明. 更重要的是：以上的证明方法不仅适用于上述一个定理，而且还适用于同该定理相似的无数定理，而与此相反，在欧几里得风格和笛卡儿风格的证明中，每个定理都需要特殊的证明方法. 我们应该感谢大卫 · 希尔伯特，是他开创了上述的具有广泛应用的普遍方法.

几何定理证明的希尔伯特风格时代

从以上可以看出希尔伯特的方法提供了几何定理证明的崭新方式，这也标志着几何定理证明的发展进入了第三个阶段.

阶段 III. 希尔伯特风格的几何定理证明 在希尔伯特的方法中，通过计算来证明的特性 (1)′, 与第二个阶段的笛卡儿方法完全一样，但是特性 (2) 却变成了以下的特性 (2)′:

(2)′ 定理的证明不再是针对某一个定理，而是针对某一类定理，也就是说，一个方法可以解决具有相似特性的所有同一类定理的证明.

§2.2 计算机时代的几何定理证明

在深入讨论希尔伯特风格的几何定理证明在计算机时代的飞跃发展之前，我们先作一些有关的评注.

<u>几何定理证明希尔伯特类的扩展</u>

我们首先指出：在 §2.1 中给出的高斯线定理的希尔伯特方式的证明已经说明了，能够用希尔伯特通用方法来证明的构造性纯交点定理类或希尔伯特类可以扩大到包括高斯定理在内的更广泛的类. 事实上，王东明首次指出：如果假设条件的安排使约束变量可以作为参数及已经引入的约束变量的有理函数而依次引入的话，那么 §2.1 所述的希尔伯特通用方法就可以扩展到包括与垂线甚至与圆有关的一些定理. 王用这种方式证明了许多非平凡的有趣定理，这方面的工作可参阅 [W-G]. 最近陆、李等人又将这个类进一步扩展到包括欧几里得几何中所有有意义的定理，参看 §7.2.

<u>希尔伯特类的构造定理</u>

如前所述希尔伯特最初的方法有很大的局限性，这一方面是因为它考虑的类只能包括涉及关联性和平行性的定理 (尽管王东明等人已作了很大的扩展)，另一个方面则是因为定理应具有 *构造性* 特征，即点与线，或者说约束变量应当是依次逐个引进. 这样做起来也许不容易，即使我们将定理限制在仅涉及关联性和平行性的范围内. 这一点可以由下面的例子看出 (这个例子属于 Bokowski).

例 2.2.1 考虑图 2.7. 数字 1, 2,···, 8 代表普通三维空间中的八个点. 这个图形中由四个点如 1, 2, 5, 6 为顶点的正方形称为共面的，如果相应于 1, 2, 5 和 6 的四个空间点是共面的. 由此可以得出：

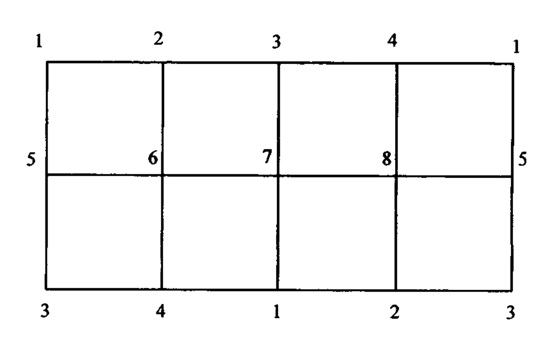


图 2.7 Bokowski 的例子

Bokowski 定理 在图 2.7 中如果八个正方形中有七个是共面的，则第八个也是共面的.

至少表面上看来，对上述推测很难给出构造性证明，希尔伯特方法在这里很难应用 (虽然最终证明它是可行的). 这方面的其他例子可以看 §7.3 例 7.3.1 和论文 [WWT3] 中的例 7.

希尔伯特通用方法的非退化条件

现在让我们来进一步考察希尔伯特的通用方法证明过程中出现的非退化条件 (1.3),(1,7) 和具有非零分母的 (1.8) 式. 由第 1 节中关于 Desargues 定理的证明可以看出，非退化条件在待证定理的陈述中通常都没有明确交待. 为了说明这一事实的严重性，现摘引著者一篇论文 [WWT3] 中的一段话如下：

…… 通常几何中几乎所有的定理都只能说是一般性成立，或者说仅在某些非退化条件下成立，而这些非退化条件在定理中往往并没有被明确说明. 这一事实对于我们所相信的定理证明的欧几里得方法的严格性来说至关重要，因为我们难于清楚地表述那些需要满足的非退化条件，同时我们难于检验所讨论的定理证明过程中需要用到的老定理是否属于使它们不能成立的退化情形.

希尔伯特风格的几何定理证明的机械化特征

虽然可以用希尔伯特方法证明的定理类范围有限，但这种方法的重要性仍然无可估量. 不是一条一条定理证明，而是以一个通用的方法同时证明一整类定理，固然是其新颖之处，但除此之外证明方法本身也是完全新颖的：它具有机械化的特征，即人们只要一步一步地按照指令进行，就能达到需要证明的定理的最后结论. 为了认识希尔伯特方法的价值，下面摘引著者论文 [WWT2] 中的一段：

希尔伯特 1899 年的经典著作《几何基础》是数学公理化的代表，它奠定了欧几里得几何的严格基础，这方面的巨大功绩已为世人所公认. 然而，人们迄今为止很少注意到这部经典还有另一项 (在著者看来也许是更伟大的) 功绩. 事实上，这部经典著作也是几何机械化的代表，同时指明了实现机械化目标的道路.

顺便指出，由于前述非退化条件的出现，所谓“严格基础”尚值得推敲.

根据希尔伯特方法的机械化特征，我们重新陈述希尔伯特经典著作中的定理 62 如下：

希尔伯特机械化定理 平面上构造性纯交点定理的希尔伯特类是可以机

械化的.

几何定理证明的计算机阶段

20 世纪 40 年代计算机的出现极大地推动了希尔伯特风格的几何定理证明的发展. 实际上, 定理证明的希尔伯特方法之机械化特征使我们得以将定理证明过程直接转化为能在计算机上运行的程序, 来检验该定理是否正确. 于是在计算机上运行计算本身就成为对该定理的证明或否定. 由于计算机这一强有力的工具, 几何定理证明进入了使用计算机为证明工具的第四个发展阶段.

阶段 IV. 计算机风格的几何定理证明 在这个阶段特征 (1)′ 被进一步加强为

(1)″ 定理证明是在 计算机 上通过计算完成.

整类整类地证明定理的特征 (2)′ 则没有发生变化. 顺便强调指出, Haken 在计算机上完成的四色定理证明不能被认为是属于这一风格的定理证明, 因为这个证明只适用于这一单个的定理, 这不符合特征 (2)′. 因此, 尽管 Haken 完成的这个证明价值无可估量, 但按著者的看法它仍然只能算作是欧几里得或者笛卡儿风格下的一个证明.

机械化定理证明

随着计算机的出现, 人们很自然地想到如何将一定类型定理的证明过程转化为能在计算机上执行的程序, 而这种算法证明过程的存在性正如希尔伯特类的情形那样已经在某种意义上得到保证. 情况也确实如此. 20 世纪 50 年代出现了一个运用计算机来进行几何定理证明的认真的尝试阶段, 并终于导致了 60 年代初的突破. 中国数理逻辑学家王浩 (+1921, +1995), 在 IBM 704 型计算机上只用 3 分钟的时间证明了约二百条有关命题演算的定理, 参阅 [WH1]. 这项先驱性成就被人们恰当地誉为"一箭七雕", 王浩因此于 1983 年获得了首届机械化或自动定理证明奖.

王浩对几何定理证明由欧几里得风格阶段到今天运用计算机阶段的发展作了精彩的概括 (参阅 [WH2], p.106):

使用计算机来帮助数学发现最基本的问题就是要寻找有效的方法将定性的困难转化为定量的复杂性.

几何定理证明的定性困难在很大程度上已由笛卡儿和希尔伯特的方法而得到克服, 而定量复杂性问题则将通过计算机的使用来解决. 王浩的成功激起了人们寻求用计算机证明有意义的定理的更强有力的方法的巨大努力. 60 年代以来已出现了为实现这一目标的各种结果与方法. 这方面的概述可参阅

[B-L].

然而，所有上述成就尽管具有重大的理论意义，却很少能引起在第一线工作的数学家们的兴趣. 从数学家的观点看， Tarski 在 1950 年发现的一条定理具有重要意义. 与希尔伯特机械化定理相比较，我们将仍然称 Tarski 定理为机械化定理:

Tarski 机械化定理 通常意义下的初等几何是可以机械化的.

看一看在计算机上运用 Tarski 机械化定理的方法究竟能做些什么，一定很有意思. 然而结果似乎令人失望. Tarski 的方法过于复杂，效率低下，以致于迄今还未能用这种方法在现代大型计算机上证明什么有意义的几何定理.

<u>近年来有关机械化几何定理证明的研究</u>

在 1977 年本书作者发现了一种证明几何定理的普遍方法，该方法适用于甚至是经过扩充的希尔伯特类中的所有定理以及 Tarski 类中的部分 (但非全部) 定理. 该方法效率颇高，人们已经用它证明甚至发现了几百条有意义的定理. 我们将在以后的章节，尤其是第七章中，对机械化几何定理证明领域所做的工作进行详细的介绍.

§2.3 古代中国的几何问题求解和几何定理证明

<u>中国古代的几何问题求解</u>

中国古代的几何有较好的发展，但在某些方面与欧几里得几何有很大的不同. 实际上，鉴于古希腊非常重视几何定理证明的研究，人们通常将古中国的几何研究视为问题求解而不是定理证明. 大量的几何问题来自于实践要求. 现举例如下:

1. 来自实际测量中的问题，例如，测量太阳的地面高度或参照标高 (或标杆) 测量山的海拔高度.

2. 面积和体积的测量. 值得注意的是秦九韶在《数书九章》(1249 A.D.) 中提出的由三边求三角形面积的公式，是海伦公式的另一种形式.

3. 与勾股形 (也就是直角三角形) 相关的问题，例如: 有理比例的勾股数的确定.

4. 来自于实际生活的问题，例如: 通过某种方式的步测来确定城市或耕地的长宽尺寸.

总之，古代中国几何学的发展是面向应用的，这与欧几里得几何强调逻辑基础及逻辑关系的发展方向形成鲜明对照. 但是这并不意味着古代中国没有

发展几何定理证明. 事实上, 古代中国长期形成了一些简单适用的原理而不是一系列公理, 然后以公式的形式给出几何定理的证明或通过逻辑推理来解决几何问题.

出入相补原理

下面也许是最简单的一条原理.

出入相补原理 当把一个平面 (或立体) 图形分割成若干块, 各块移动并重新拼合后, 整个图形的面积 (或体积) 保持不变.

这条看似简单的原理, 已经被以一种优美的, 往往令人惊异的方式应用于多种几何问题的求解和几何定理的证明. 上述 (1)~(4) 类问题中绝大部分公式都是以此原理为基础得以证明的.

勾股定理

中国古时候将直角三角形称为勾股形. 直角的短边称为勾, 长边为股, 斜边为弦. 古代中国的数学家对勾股形非常感兴趣, 以此为核心构筑了传统的几何学. 因此毕达哥拉斯定理在我们的词语中应称勾股定理.

整个《九章算术》第九章都在讨论勾股定理及其应用, 共包含了 24 个问题. 下面是问题 1 (其中尺为长度单位, 3 尺 = 1 米).

问题 1. 今有勾三尺, 股四尺, 问弦为几何?

答曰: 五尺.

勾股术曰: 勾股各自乘, 并而开方除之, 即弦.

刘徽在《注释》中首先如上述那样定义了勾股弦, 然后以出入相补原理为基础对结论给出了一个证明. 从刘徽的注释可以看出, 原文曾有一张附图, 图中有以勾为边的红色正方形和以股为边的蓝色正方形. 请注意该题证明和叙述中的特殊三元数组 (3, 4, 5) 仅仅是作为解释性的例子, 一如中国古代文献的传统, 它具有超越特殊数据的一般特性. 关于这点请参见 §1.1.

古代中国的测量仪器——矩

人们一定在很古远的年代就了解勾股定理了. 在说明这一点之前让我们首先来看看 矩 这种在古代中国广泛使用的测量仪器.

矩 由成直角的双臂构成, 在勾股之一臂或两臂上标有刻度. 在《周髀》中有一段学者商高答周公问:

平矩以正绳, 偃矩以望高, 覆矩以测深, 卧矩以知远, 环矩以为圆, 合矩以为方.

周公是中国历史上非常有名的政治家, 他推翻了商朝, 在公元前 1122 年

建立了西周. 至于商高, 在陕西省的地方志中有一些关于他的历史记载.

《周髀》中的勾股定理

在《周髀》中有一段商高和周公关于勾股定理的对话. 对话中提到了特殊的三元组 (3, 4, 5), 但正如我们前面已多次指出的那样, 这只是一种示例. 这段对话中有几句话以前一直难于理解. 幸好陈良佐, 李国伟 (台湾) 和李继闵 (大陆) 教授在最近的研究中分析了这段话的意思, 他们得出结论证实那几句话可以看成是一般勾股定理的证明, 尽管不是太严格. 三国时期的赵爽 (约公元 3 世纪) 对《周髀》作了注释, 赵爽注形成了本书第一章第一节中提到的两篇独立的文章 [ZS1]* 和 [ZS2]*. [ZS1]* 还有一些彩色附图也幸存至今. 利用了这些年代久远的附图, 同时也由于对原文中一些文字的恰当理解, 上面提到的几位数学家建议了一个看来是符合古代原证的勾股定理证明. 下面的图 2.8 引自文献 [LJM1]*.

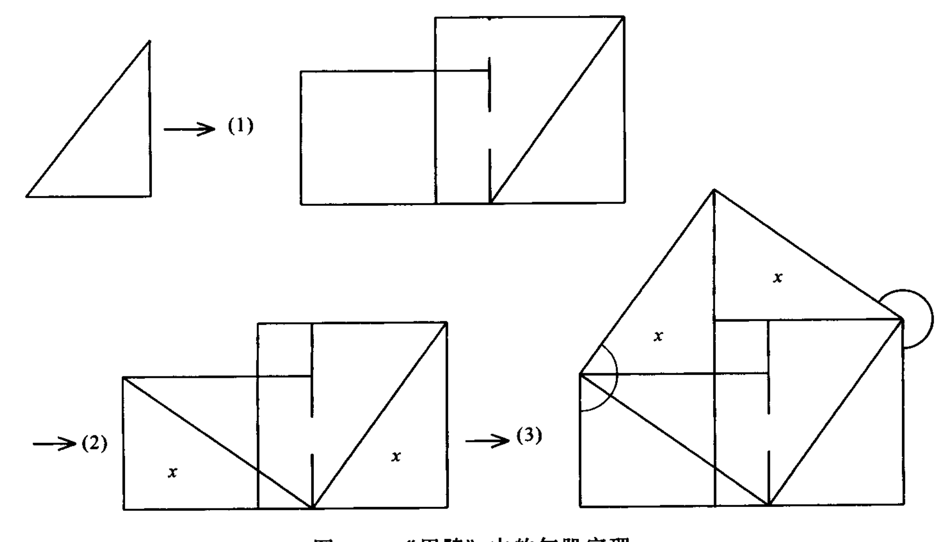


图 2.8 《周髀》中的勾股定理

在图 2.8 中, 图 (1), (2), (3) 分别对应下面的陈述 (其中序号 1, 2, 3 为作者所加):

(1) 既方之.

(2) 外半其一矩.

(3) 环而共盘, 得成三, 四, 五.

《周髀》中的日高公式

在《周髀》中还有另一项非常重要的几何结果, 后来被进一步发展为更

精确的形式，现介绍如下.

在南北方向的一条直线上放置两根有一定间距的表. 在中午时测量两表的影长，那么太阳的地平面高度将由以下公式给出：

日高公式

$$\text{日高} = \frac{\text{表距} * \text{表高}}{\text{影差}} + \text{表高}. \tag{2.3.16}$$

《周髀》中给出的数据过于粗疏而与实际不符. 然而，正是以这一公式为基础，古人建造了一种以周公命名的测影台. 今天在河南省仍然保存着这样一座测影台，该测影台被认为是周公时代的建筑，但实际上是元代著名天文学家、数学家和工程师郭守敬 (+1213, +1316) 所重建.

《周髀》中并没有这一公式的证明. 现在的许多证明都是通过作一些辅助平行线，然后用欧几里得几何的方式来推导. 请参见图 2.9.

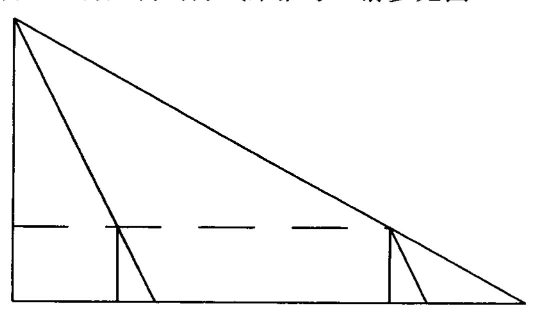


图 2.9 日高公式

然而，这样的证明决不可能是古代的证明. 事实上，古代中国几乎没有注意到平行的概念，在明或最多在元朝才出现欧几里得几何的痕迹.

<u>日高公式的复原</u>

所幸的是，在赵爽所著的《周髀》注中有一篇文章 [ZS2]* 以及一张彩色的日高图. 本书作者给出了一个证明. 这个证明即使不是赵爽的原证，也会是非常相近. 为此，下面我们先给出文章 [ZS2]* 中一些段落的字面翻译，其中的句子已经重新排序，序号 (1)~(9) 为作者所加.

(1) 黄甲与黄乙其实正等.

(2) 黄甲与青丙相连，黄乙与青己相连.

(3) 其实亦等.

(4) 青丙与青己其实亦等.

(5) 以表高乘两表相去为黄甲之实.

(6) 以影差为黄乙之宽.

(7) 而一，所得则变得黄乙之袤 (móu).

(8) 上与日齐.

(9) 按图当加表高.

根据上面的说明我们可以补出原图，大致如图 2.10.

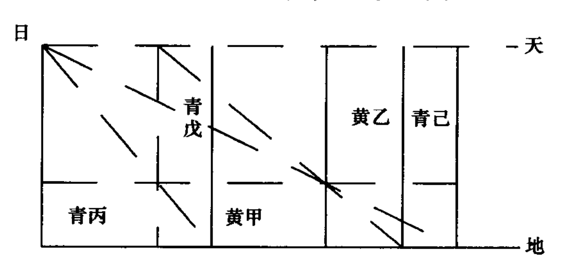


图 2.10 日高公式的复原

现在证明已变得十分清楚. 事实上，作为出入相补原理的一个简单结果，从 (1),(2),(3) 我们有以下的面积等式：

$$黄甲 = 黄乙, \qquad 青丙 + 黄甲 = 青己 + 黄乙.$$

由此我们有 (4)：

$$青丙 = 青己.$$

同样我们有青丙 = 青戊，由此得

$$青戊 = 青己.$$

由 (5) 可得

$$面积\ Y_1 = 表距 * 表高.$$

由 (1) 可知这也是 Y_2 的面积. 于是

$$\begin{aligned} 黄乙\ 宽 &= (黄乙 + 青己)宽 - 青己\ 宽 \\ &= (黄乙 + 青己)\ 宽 - 青戊宽, \end{aligned}$$

由此我们有 (6), 即

$$黄乙 = 影差.$$

如 (7) 和 (8) 所示，我们进一步得：

$$\begin{aligned} 表以上日高 &= \frac{黄乙面积}{黄乙宽} \\ &= \frac{表高 * 表距}{影差}. \end{aligned}$$

正如 (9) 所示，我们有

$$\text{地平面上日高} = \text{表以上日高} + \text{表高},$$

这就是公式 (2.3.16).

城宽问题

§1.2 中所描述的将《九章算术》中的城宽问题化为带从开平方问题 (图 1.5 和图 1.6) 之过程可以根据出入相补原理证明如下：

我们先将图 1.5 及图 1.6 合并成图 2.11. 由出入相补原理我们有矩形 PR 面积 = 矩形 QS 面积 $= w*n$. 矩形 RT 的面积为 $2*w*n$, 两边的差为 $n+s$. 因此矩形的宽，即城宽，可以如前述那样通过以 $2*w*n$ 为实， $w+s$ 为从开方而得到.

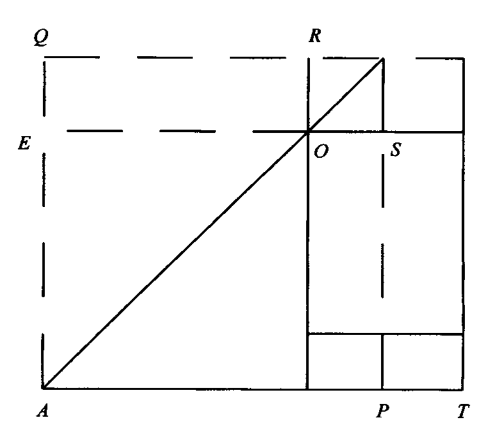


图 2.11 城宽问题

出入相补原理对勾股形研究的应用

出入相补原理的应用是多方面的. 除了开平方外，还有勾股定理的证明，日高公式的证明，等. 下面我们再举两个应用的例子 (1) 和 (2), 它们来自《九章算术》的勾股章，参见 [WWT1]*.

(1) 勾股问题：在 勾±股, 弦±勾, 弦±股, 勾, 股, 和弦中, 假设有两个已知，求其他各项. 例如，让我们来考虑折竹问题 13. 刘徽 注 首先将这个问题转化成一个从 勾 和 弦±股 决定 弦 和 股 的问题. 然后给出如下公式形式的解：

$$\text{股} = \frac{(\text{弦}+\text{股})^2 - \text{勾}^2}{2*(\text{弦}+\text{股})}, \tag{2.3.17}$$

$$\text{弦} = (\text{弦}+\text{股}) - \text{股}.$$

刘徽的证明完全是几何的，基于出入相补原理. 请参见图 2.12.

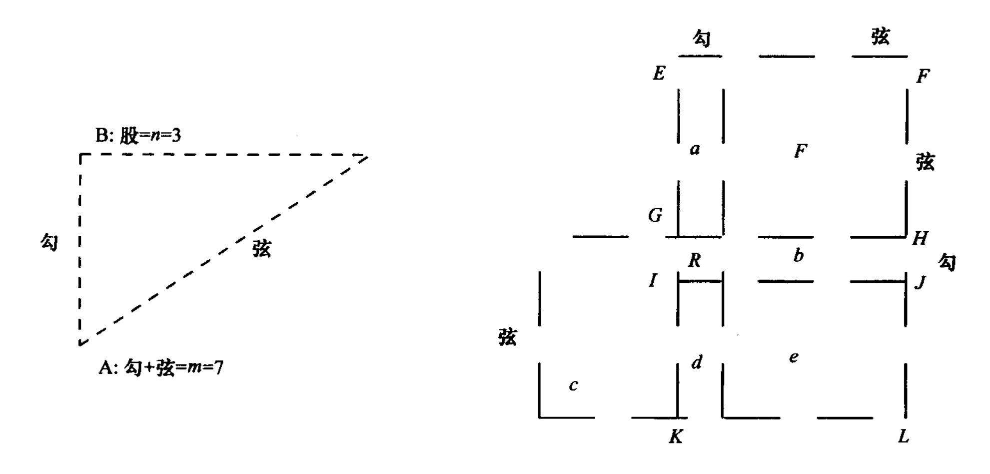


图 2.12 勾股章中两个应用的例子

(2) 勾股数.

《九章算术》勾股章问题 14 以最一般的形式给出了有理勾股数组. 问题如下：

问题 14

今有二人同所立.

甲行率七，乙行率三.

乙东行；甲南行十步而邪东北与乙会.

问甲、乙行各几何？

答曰：

乙东行一十步半；甲邪行一十四步半及之.

术曰：

令七自乘，三亦自乘，并而半之，以为甲邪行率.

邪行率减于七自乘，余为南行率.

以三乘七为乙东行率.

正如以前多次提到的，术中具体的数值 3, 7 并不重要. 我们可以将 3, 7 用 n, m 来代替，有

$$n = 勾, \quad m = 勾 + 弦, \tag{2.3.18}$$

见图 2.12. 在 (2.3.17) 中让我们将勾和股交换，然后乘以 $2 * (弦 + 勾)$, 很容易

得到以下的有理勾股数组的一般公式：

$$勾:股:弦 = \left[m^2 - \frac{(m^2+n^2)}{2}\right] : m*n : \frac{m^2+n^2}{2}. \tag{2.3.19}$$

注释 2.3.1 《九章算术》的第九章中给出了 8 组有理勾股数，即

3 : 4 : 5, 5 : 12 : 13, 7 : 24 : 25, 8 : 15 : 17, 20 : 21 : 29, 48 : 55 : 73, 60 : 91 : 109, 20 : 99 : 101.

这表明当时的数学家应该已经知道推导勾股数的一般方法了. 事实上，这些勾股数组分别对应于公式 (2.3.19) 中：

$m:n = 2:1, 3:2, 4:3, 5:3, 7:3, 11:5, 13:7$和$11:9$.

上述问题 14 则相当于 $m:n = 7:3$ 的情形. 更进一步唐初的经典著作 [WXT]* 中出现了另外 3 组勾股数 9 : 40 : 41, 12 : 35 : 37, 13 : 84 : 85, 它们分别对应于 $m:n = 5:4, 7:5, 7:6$.

注释 2.3.2 《九章算术》中的问题 14 实际上给出了勾股数推导的一般性公式，这一点由李继闵首先指出，详见 [LJM1,2]*.

刘徽的《海岛算经》

公元 263 年，刘徽的《海岛》介绍了用 矩 来进行测量的方法. 这部著作包含了 9 个问题：

问题 1. 望岛.

问题 2. 望松.

问题 3. 望邑.

问题 4. 望谷.

问题 5. 望楼.

问题 6. 望渡口.

问题 7. 望清渊.

问题 8. 望津.

问题 9. 临邑.

每一个问题中的数据都是用 矩 从不同的测点测得的. 有时也使用绳和表. 利用这些数据，得到了一些明确的但形式复杂的测量公式. 特别需要指出的是问题 1 就是《周髀》中的日高测量. 只不过其中的太阳被海岛所代替，测量则是在海岸上进行. 这使问题变得更加实际. 近年来，一些中国数学史学家根据现存的史料记载认为刘徽著作中提到数据与山东省某地相合，参考 [Guo3]*.

但是这些测量公式是如何得到的并不清楚. 清代一些数学家通过添加辅助平行线的办法给出了欧几里得式的证明, 但是这些证明非常复杂, 很不自然. 而且很难将他们用这种方法得到的结果转化成《海岛》中给出的形式. 另一方面, 本书作者曾试图利用出入相补原理来复原古代的证明. 结果表面所复原的证明不仅简洁漂亮, 而且直接导致《海岛》中那些复杂的公式. 因此我们相信我们复原的证明就是已经失传的古代的证明, 或至少是十分接近于古代原证. 参见 [WWT2]*.

<u>秦九韶–海伦三角形面积公式</u>

公元 1247 年, 秦九韶在《数书九章》([QJS]*) 中提到一个求不等边三角形面积的问题.

秦将不等边三角形的三边命名为大斜, 中斜和小斜, 以下简记为长, 中, 短. 秦的结果可以表示成如下的公式:

$$\text{面积}^2 = \frac{1}{4} * \left[\text{短}^2 * \text{长}^2 - \left(\frac{\text{长}^2 + \text{短}^2 - \text{中}^2}{2}\right)\right]^2. \qquad (2.3.20)$$

秦并没有提到这个公式的来源. 该公式的证明也没有传下来. 利用刘徽《注释》中的结果和方法, 我们可以大致推导这一失传的证明如下 (见图 2.13):

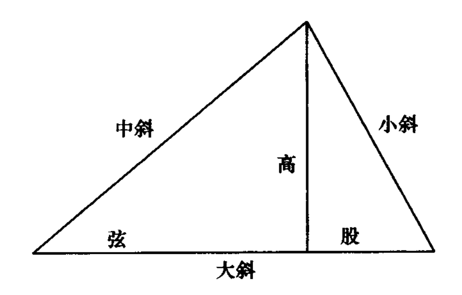


图 2.13 秦九韶 – 海伦三角形面积公式

在三角形的长边上作三角形的高, 将长边分成二部分, 将长短两部分分别作为一个直角三角形的 弦 和 股. 由《九章算术》可知该三角形的面积为 $\frac{1}{2}*$ 高 $*$ 长边, 因此我们的问题可转化成求 高, 然后又进一步归结为求该直角三角形的 股.

由于

$$\text{弦} + \text{股} = \text{长},$$
$$\text{勾}^2 = \text{弦}^2 - \text{股}^2 = \text{中}^2 - \text{短}^2,$$

我们的问题相当于：给定 勾 及 弦股 和，求 股. 由刘徽的公式 (3.2) 我们有

$$股 = \frac{(弦+股)^2 - 勾^2}{2*(弦+股)} = \frac{长^2 - (中^2 - 短^2)}{2*长},$$

$$高^2 = 短^2 - 股^2 = 短^2 - \left(\frac{长^2 + 短^2 - 中^2}{2*长}\right)^2.$$

由此我们得到秦的公式 (2.3.20).

注释 2.3.3 秦的公式看起来非常古怪. 但上述证明却非常自然，与古代中国的几何传统密合. 我们可以认为这就是原证，参见 [WWT3]*. 然而西方几何的海伦公式形式简洁漂亮，见第一章例1.2. 一旦一个简洁的公式被发现，人们不大可能再将之转变成丑陋的形式. 因此秦的公式不可能是来自海伦公式，我们可以断言它是独立于海伦公式而得出来的.

注释 2.3.4 本书作者感谢杭州大学沈康身教授及内蒙古师范大学李迪教授，他们指出了已有研究认为上述证明在清代学者梅文鼎 (+1633 ~ +1721) 的著作《三角举要》 (+1684) 中已经出现.

<u>古代中国的面积和体积理论</u>

为了丈量土地和测定容量，最重要的问题就是如何决定一个平面图形的面积和一个立体的体积. 因此面积和体积的研究占据了古代中国几何研究的核心地位也就不足为奇了.

很容易运用出入相补原理来得到三角形面积 A 的一般性公式：

$$A = \frac{1}{2} * s * h, \tag{2.3.21}$$

这里 s 是三角形的一条边， h 是相应的高. 于是无论多么复杂的多边形的面积都可以用出入相补原理来得出. 由此可见，仅仅依靠这条简明适用的原理就可以建立起多边形面积理论. 然而，对空间多面体的体积来说，情况就远非如此简单了.

<u>多面体体积的刘徽原理</u>

建立满意的多面体体积理论的关键是要证明类似于 (2.3.21) 的四面体体积公式：

$$V = \frac{1}{3} * B * h, \tag{2.3.22}$$

这里 B 为四面体一底的面积， h 为相应的高. 值得注意的是 (2.3.21) 不能单靠出入相补原理来证明，对此刘徽是十分了解的，并在其九章《注释》中完全地解决了这一难题. 刘徽的论证如下：将一个长方体斜分为两个相等的部分，并称它们为“羡除”. 再将其中一个斜分为二，有矩形底面的部分叫做阳马；另一部分叫“鳖”是有三条边互相垂直的四面体，参见图 2.14.

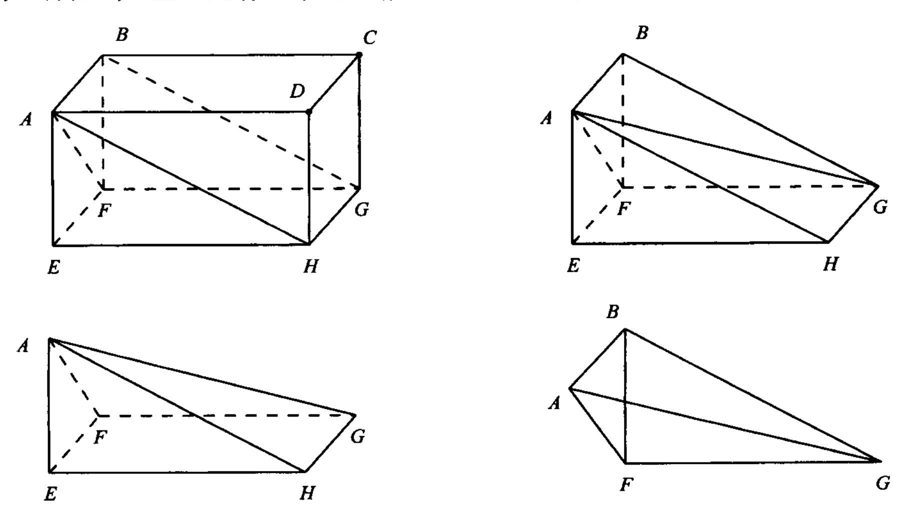


图 2.14 多面体体积的刘徽原理 a

通过将大的阳马和鳖切割成较小的阳马、鳖 (见图 2.15), 刘徽证明了：

$$1\text{ 阳马 } - 2\text{ 鳖 } = 2*(1\text{ 阳马 } - 2\text{ 鳖 }). \qquad (2.3.23)$$

不断地分割下去，式 (2.3.23) 括号中的表达式的值会越来越小，直至可以忽略不计. 正如刘徽所言：

半之弥少，其余弥细，至细曰微，微则无形，由是言之，安取余哉？

据此由 (2.3.23) 可推出如下公式：

$$\text{阳马} : \text{鳖命} = 2 : 1. \qquad (2.3.24)$$

因此，刘徽得出了一条普遍的原理，为了纪念他，我们用他的名字来命名

刘徽 2 : 1 原理

阳马居二，鳖居一，不易之率也.

注释 2.3.5 Wagner 第一个指出刘徽实际上给出了 2 : 1 原理的证明，详见他的重要文章 [Wag]*, 亦可参见 [LJM2]*.

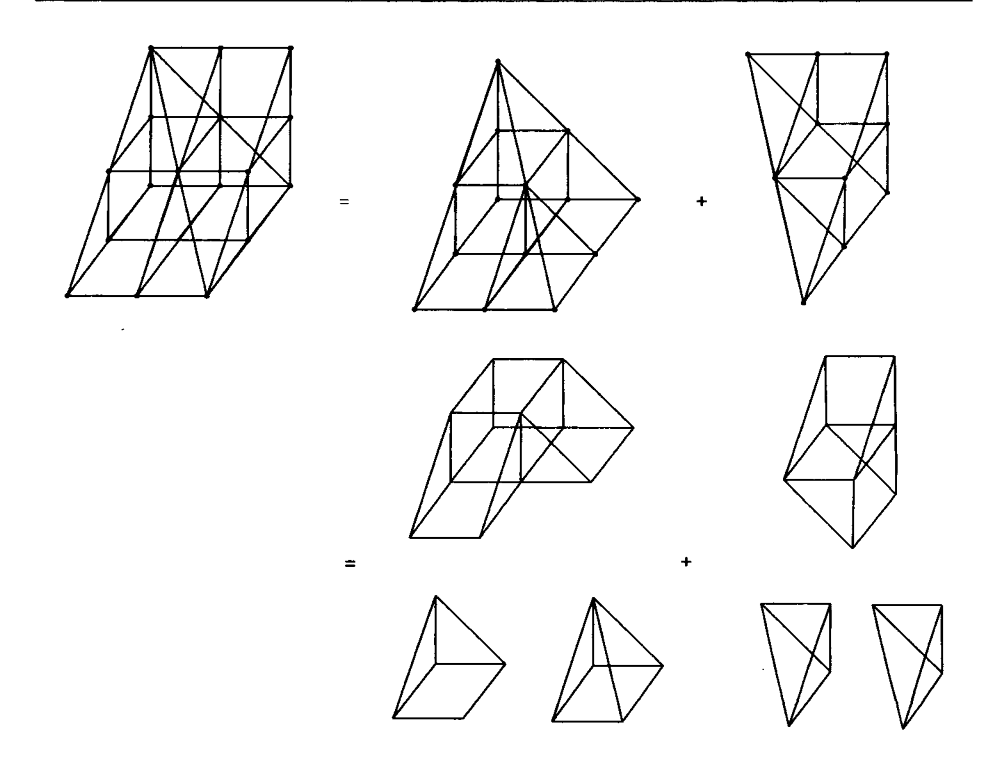


图 2.15 多面体体积的刘徽原理 b

在刘徽原理基础上，结合出入相补原理，很容易建立四面体的体积公式 (2.3.22). 而由 (2.3.22) 又可以容易地导出各种多面体的体积公式. 实际上，在《九章算术》中有许多这样的漂亮公式.

刘-祖原理

对于求由曲面围成的立体体积 (及平面曲边形面积) 来说，以上原理显然已不敷运用. 因此，已知直径来求球体积的问题在我们历史的早期一直悬而未决. 刘徽在九章注中曾建议研究一种特殊的立体，即一个正方体内两不同方向的内切圆柱相交而成的图形，并相信这方面的研究将导致球体积问题的最终解决. 然而，这个难题经过了很长时间才被伟大科学家祖冲之 (+429, +500) 的儿子祖暅所攻克. 在问题解决过程中祖暅提出了如下原理:

祖暅原理

幂势既同，则积不容异.

祖暅原理原则上给出了求由曲面围成的立体体积的一般方法. 在刘徽的《九章注》的影响下，祖暅成功地给出了球的体积的求解方法. 实际上，

祖暅原理，或更确切地说刘－祖原理，在求解简单曲面围成的立体体积时已经被刘徽所运用了，不过刘徽没有明确陈述这一原理.

注释 2.3.6 正如人们所知道的，这一著名原理在 17 世纪以 Cavalieri 原理的名称出现，它被广泛地应用于求解各种曲面围成的立体体积，对 17 世纪微积分的发明起到了重要的推动作用.

<u>古代中国面积体积理论的一般原理总结</u>

我们已经介绍了三条几何问题求解的一般原理，尤其是关于平面及立体几何图形的面积和体积理论的建立，这三条原理是：

Ⅰ. 出入相补原理；

Ⅱ. 刘徽 2 : 1 原理；

Ⅲ. 祖暅或刘－祖原理.

总之：原理Ⅰ足以建立多边形面积理论. 原理Ⅰ，Ⅱ结合起来足以建立起令人满意的多面体体积理论. 原理Ⅰ，Ⅱ及Ⅲ合起来原则上可以给出任意曲面围成的立体体积的求解方法.

<u>西方世界的体积理论</u>

与希尔伯特 1899 的经典著作《几何基础》中的面积和体积理论作一番比较是非常有趣的. 希尔伯特以所谓剖分相等概念 (Zerlegungs-aequivalenz, 与出入相补原理相似) 为基础，给出了建立多边形面积理论的方法. 然而，这个方法对于多面体体积的情形就不适用，有关的探讨构成了希尔伯特 23 个著名的数学问题中的问题 3(1900). 该问题当年即被 M.Dehn 攻克，参见 [Dehn1]. Dehn 给出了两个多面体 *剖分相等* 的充分条件，参见 [Dehn2]. Dehn 的工作晚些时候被 J. P. Sydler 所改进，Sydler 证明 Dehn 条件不仅是充分的，而且也是必要的，参见 [Syd]. Dehn 条件的表述非常复杂. 另外，在希尔伯特 1899 年的经典工作之后不久，许多发表在数学年鉴 (Mathematische Annalen) 上的文章表明：要建立一个令人满意的多面体体积理论，某种极限的概念似乎是不可避免的. 多面体体积问题是一个非平易的问题. 将刘徽的方法与希尔伯特 Dehn-Sydler 的方法相比较，作者认为刘徽的体积理论是整个数学史上最基本，最重要，和最漂亮的杰作之一.

<u>古代中国 π 的计算</u>

对测量而言，知道圆周和直径的比，即确定 π 值也是非常重要的. 从已有的史料看，社会生产力和科学技术水平越是发展，π 的计算精度要求也越高. 下面我们列出一些已知的中国古代得到的 π 值：

在汉朝以前，有“周三径一”，即 $\pi = 3$；

新莽时期 (+ 9~+23) 官定铜制圆柱形标准量器“律嘉量斛”的铭文记载 $\pi = 3.1547$；

天文学家张衡 (+78~+139) 在其《灵宪》一书中取 $\pi = \frac{730}{232}$ 或 3.1466；

张衡的球体积公式中 $\pi = \sqrt{10}$ 或 3.1622；

王蕃 (+ 219~+287):$\pi = \frac{142}{45}$ 或 3.1556.

所有以上结果似乎都是经验性的，缺乏理论基础.

又是刘徽在他的《九章注》中指出了获得尽可能精确的 π 值的一般方法. 他指出 $\pi = 3$ 这一极其粗略的估值仅仅是圆内接正六边形的周长与直径之比. 他证明从内接正六边形开始，边数不断加倍，就会得到越来越精确的比值. 而且，误差将小于那些正多边形边上的矩形面积之和. 为了理解刘徽的有关注文，可参见图 2.16.

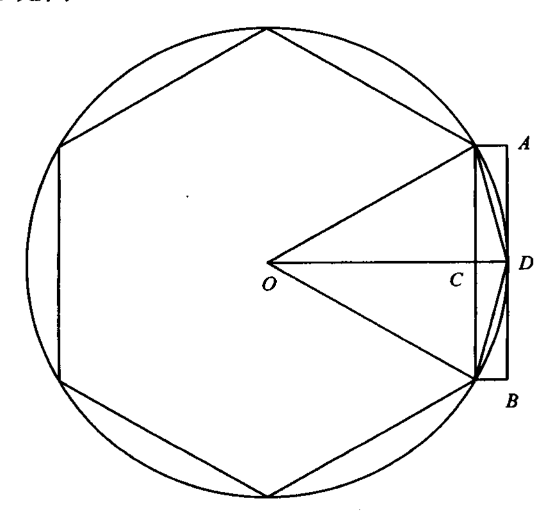


图 2.16　古代中国 π 的计算

在当边数达到 $3 * 2^6 = 192$, 刘徽给出了圆周率的近似值 $> 3.14\frac{64}{625}$ (或 3.141024) 和 $< 3.14\frac{169}{625}$. 如果边数取 $3 * 2^{10} = 3072$, 近似值将会略小于 $\frac{3927}{1250}$ (或 3.1416).

刘徽方法最重要的意义在于它包含的极限概念. 实际上，刘徽说道：

割之弥细，所失弥少. 割之又割以至于不可割则与圆合体而无所失矣.

与刘徽在建立 2 : 1 原理时说过的话相比较我们可以看出他已经有了一幅关于极限概念和极限过程的非常清晰的图像.

公元 5 世纪伟大的科学家祖冲之给出了 π 值的范围为

$$3.1415926 < \pi < 3.1415927$$

即《隋书》“律历志”所称“正数在盈朒二限之间”.

据《隋书》“律历志”记载祖冲之还得到圆周率的另外二个近似值 $\pi \approx \frac{22}{7}$ 和 $\pi \approx \frac{355}{117}$, 分别称之为 *约率* 和 *密率*. 祖冲之关于 π 的计算及其他一些重要成就都记录在《缀术》一书中. 不幸的是这本书很久以前就失传了, 现在已无法判断祖冲之是如何得到其 π 值了. 如果祖冲之采用的是刘徽的方法, 那么他必须算到 $3 * 2^{12} = 12,288$ 和 $3 * 2^{13} = 24,576$ 边形, 才能得到前述的“盈”、“朒”之数.

注释 2.3.7 $\frac{355}{117}$ 是分子分母在 1000 以下最接近 π 的分数. 大约 1000 年以后欧洲的 Otto(德国) 和 Antonisz(荷兰) 才得出相同的结果, 因此在西方数学中称其为 Antonisz 率.

注释 2.3.8 据《隋书》“律历志”记载祖冲之还得到圆周率的另外二个近似值 $\pi \approx \frac{22}{7}$ 和 $\pi \approx \frac{355}{117}$, 分别称之为 *约率* 和 *密率*. 对于祖冲之如何得出这两个分数值, 特别是 *密率*, 在数学史上还是一个谜.

<u>宋 - 元时期几何的代数化</u>

通过《海岛算经》诸公式以及秦九韶 - 海伦公式证明的复原, 我们可以看到中国古代几何强烈的代数特征. 这种代数特征在宋元时期发明的“天元术”与“四元术”中发展为系统的方法. 事实上, 通过设某些未知的几何量为“天元”、“地元”等 (相当于今天的未知数记号 x, y 等), 其他几何量就可以转化为我们今天所说的多项式, 而几何关系就转化成关于“天元” (或 x) 等的多项式方程. 李冶的两本书 [LY1,2]* 就是致力于天元术的应用的.

据传宋元时期曾出现过一些著作, 讨论如何将天元术推广为涉及二元, 三元, 甚至四元 (相当于二个, 三个或四个未知量) 的方法. 除了朱世杰的两本书 [Zhu1,2]*(+1299, +1303) 很幸运地保存下来外, 其他的书都已经失传了. [ZSJ2]* 卷中第五门包含了 8 个关于勾股定理和测量的问题. 问题 1-3 是《九章算术》中城宽问题的变体. 问题 4-8 与《海岛算经》中问题 1-4, 7 比较只有很小的修改, 例如: 海岛变成了某种圆形的城市. 以上描述的《海岛算经》中公式的证明现在由方程的求解来替代.

正如第 1.2 节所述, 方程的求解在古代中国的数学中占据了中心位置, 实际上也是本书主要关心的问题.

第二部分　原理与方法

第三章　作为零点集的代数簇和特征集方法

§3.1　仿射空间和投影空间的扩张点和特定化

<u>*基本概念和记号*</u>

记号 3.1.1　令 $\mathbf{K}$ 为特征为零的基域，$\omega_1, \cdots, \omega_i, \cdots$ 为 $\mathbf{K}$ 上的独立未定元的无限序列. $\mathbf{\Omega}$ 为 $\mathbf{K}$ 上关于所有 ω_i 的有理函数域，且 $\mathbf{\Omega}^*$ 为 $\mathbf{\Omega}$ 的代数闭集.

例 3.1.2　$\mathbf{K}$ 可以是有理数域 $\mathbf{Q}$, 实数域 $\mathbf{R}$, 复数域 $\mathbf{C}$, 等等.

定义 3.1.3　称 $\mathbf{\Omega}^*$ 为 $\mathbf{K}$ 上的 *泛域*.

定义 3.1.4　$\mathbf{K}$ 的 *扩域* 是指包含在 $\mathbf{\Omega}^*$ 中的 $\mathbf{K}$ 的任一有限生成的扩域.

注释 3.1.5　引入泛域仅是为了避免在域的不断扩张中牵涉到的逻辑上的困难. 如参考文献 [H-P2], 第三卷，第十章，第一节. 实际上这并不影响后面的整个理论.

记号 3.1.6　记 $\mathbf{K}(\xi_1, \cdots, \xi_r)$ 为将 $\xi_1, \cdots, \xi_r \in \mathbf{\Omega}^*$ 加到 $\mathbf{K}$ 中所得到的扩域，即包含 $\xi_1, \cdots, \xi_r$ 的 $\mathbf{K}$ 的极小扩域.

记号 3.1.7　对 $\mathbf{K}$ 上的扩域 $\mathbf{K}^*$, 记 $\mathrm{TrDeg}(\mathbf{K}^*/\mathbf{K})$ 为扩域 $\mathbf{K}^*$ 在 $\mathbf{K}$ 上的超越次数. 即扩域 $\mathbf{K}^*$ 在 $\mathbf{K}$ 上的代数独立元的最大个数.

<u>*仿射空间和扩张点*</u>

记号 3.1.8　记 $\mathbf{K}^n$ 或 $A^n_{\mathbf{K}}$ 为 $\mathbf{K}$ 上维数为 n 的仿射空间或 n 维仿射空间.

定义 3.1.9　$\mathbf{K}^n$ 中的 *点* 是指在 $\mathbf{K}^n$ 中的元素，记作 $X = (x_1, \cdots, x_n)$, 其中 $x_i \in \mathbf{K}$ 是 X 的第 i 个坐标.

记号 3.1.10　对 $X = (x_1, \cdots, x_n)$, 记 $X_k := (x_1, \cdots, x_k)$, 其中 $0 < k \leq n$. **约定**　当 $k = 0$ 时，$X_k = X_0 :=$ 空集.

定义 3.1.11　$\mathbf{K}^n$ 中的 *扩张点* 是指 $\mathbf{K}^{*n}$ 中的点，其中 $\mathbf{K}^*$ 是 $\mathbf{K}$ 的某个扩域. $\mathbf{K}^n$ 中的 *普通点* 是指 $\mathbf{K}^n$ 中的点.

定义 3.1.12　$\mathbf{K}^n$ 中的扩张点 $\Xi = (\xi_1, \cdots, \xi_n)$ 的 *定义域* 是指 $\mathbf{K}$ 的扩域

$\mathbf{K}(\Xi) = \mathbf{K}(\xi_1, \cdots, \xi_n)$.

定义 3.1.13 $\mathbf{K}^n$ 中的扩张点 Ξ 在 $\mathbf{K}$ 上的 *维数* 定义为 $\mathrm{TrDeg}(\mathbf{K}(\Xi)/\mathbf{K})$.

记号 3.1.14 $\mathbf{K}^n$ 中的扩张点 Ξ 在 $\mathbf{K}$ 上的 *维数* 记作 $\mathrm{Dim}_{\mathbf{K}}\, \Xi$.

扩张点的典范表示

记号 3.1.15 对于 $\mathbf{K}^n$ 中的扩张点 $\Xi = (\xi_1, \cdots, \xi_n)$, 记 Ξ_i 为 $(\xi_1, \cdots, \xi_i)$, $i = 1, \cdots, n$. 当 $i = 0$ 时, $\Xi_0 :=$ 空集.

对于扩张点 $\Xi = (\xi_1, \cdots, \xi_n)$, 假设对于 $0 < i < c_1$, 每个 ξ_i 在 $\mathbf{K}(\Xi_{i-1})$ 上都是超越的, 而 ξ_{c_1} 在 $\mathbf{K}(\Xi_{c_1-1})$ 上是代数的, 其定义方程为

$$E_1 \equiv \xi_{c_1}^{d_1} + f_{11} * \xi_{c_1}^{d_1-1} + \cdots + f_{1d_1} = 0, \quad f_{1j} \in \mathbf{K}(\Xi_{c_1-1}).$$

假设对于 $c_1 < i < c_2$, 每个 ξ_i 在 $\mathbf{K}(\Xi_{i-1})$ 上都是超越的, 而 ξ_{c_2} 在 $\mathbf{K}(\Xi_{c_2-1})$ 上是代数的, 其定义方程为

$$E_2 \equiv \xi_{c_2}^{d_2} + f_{21} * \xi_{c_2}^{d_2-1} + \cdots + f_{2d_2} = 0, \quad f_{2j} \in \mathbf{K}(\Xi_{c_2-1}).$$

这个过程可以尽可能地继续下去, 从而 $\mathbf{K}^n$ 中的扩张点 $\Xi = (\xi_1, \cdots, \xi_n)$ 可以用如下的一组多项式 $E_i (i = 1, \cdots, r)$ 表示:

$$E_i \equiv x_{c_i}^{d_i} + f_{i1} * x_{c_i}^{d_i-1} + \cdots + f_{id_i},\ f_{ij} \in \mathbf{K}(X_{c_i-1}),\ j = 1, \cdots, d_i. \tag{3.1.1}$$

定义 3.1.16 对于上述的扩张点 $\Xi = (\xi_1, \cdots, \xi_n)$, (3.1.1) 中的多项式 E_i 称为 Ξ 的 *定义多项式*. 由这些 E_i 组成的集合称为 Ξ 的 *定义多项式集*. 相应的方程集 $E_i = 0$ 称为 Ξ 的 *定义方程组*. ξ_{c_i} 称为 Ξ 的 *限制坐标*, 而 $\xi_j (j \neq c_i)$ 称为 Ξ 的 *自由坐标*.

扩张点的其他表示

从域的代数扩张理论, 我们有如下引理:

引理 3.1.17 设 ξ 是 $\mathbf{K}$ 上的代数元且满足 $\mathbf{K}$ 上的如下方程:

$$E \equiv x^d + f_1 * x^{d-1} + \cdots + f_d = 0, \quad f_i \in \mathbf{K},$$

则代数扩域 $\mathbf{K}(\xi)$ 中的任意元 η 可唯一地表为如下形式:

$$\eta = \sum_{i=0}^{d-1} k_i * \xi^i,$$

其中 $k_i \in \mathbf{K}, i = 0, \cdots, d-1$.

记号 3.1.18 对于 $\Xi = (\xi_1, \cdots, \xi_n)$ 及其如 (3.1.1) 所示的定义方程 E_i, 令 $y_i := x_{c_i}; Y_i := (y_1, \cdots, y_i)$, $i = 1, \cdots, r$; $u_1, \cdots, u_{n-r} :=$ 按原来的序排列余下的 x_i; $U := (u_1, \cdots, u_{n-r})$; $U_i :=$ 出现在 X_{c_i-1} 中的 u_j 的全体, $i = 1, \cdots, r$.

对 (3.1.1) 中的方程 $E_i=0$ 不断运用引理 3.1.17, 则得到了如下命题:

命题 3.1.19　*设 η 是 $\Xi=(\xi_1,\cdots,\xi_n)$ 的定义域中的任意元，其定义多项式为 (3.1.1) 中的 E_i, 则 η 可唯一地表为如下形式:*

$$\eta=\sum_e k_e*\xi_{c_1}^{e_1}*\cdots*\xi_{c_r}^{e_r},\quad k_e\in\mathbf{K}(\Xi^{(0)}),$$

其中 $\Xi^{(0)}$ 为所有 $\xi_j(j\neq c_i)$ 组成的集合， e 取遍所有满足 $0\le e_1<d_1,\cdots,$ $0\le e_r<d_r$ 的 $(e_1,\cdots,e_r)$.

现对 E_i 中的元 f_{ij} 应用命题 3.1.19, 消去分母后，得到如下命题:

命题 3.1.20　(3.1.1) 中扩张点 $\Xi=(\xi_1,\cdots,\xi_n)$ 的定义多项式 E_i 可以写为如下形式:

$$\begin{aligned}&E_i'\equiv f_{i0}'*y_i^{d_i}+f_{i1}'*y_i^{d_i-1}+\cdots+f_{id_i}',\\ &f_{i0}'\in\mathbf{K}[U_i],\quad f_{ij}'\in\mathbf{K}[U_i,Y_{i-1}],\quad j=1,\cdots,d_i,\end{aligned}\tag{3.1.2}$$

其中对每个 f_{ij}' 和 $k<i$, f_{ij}' 关于 y_k 的次数小于 d_k. 此外，对每个 $i=1,\cdots,r$, 多项式 E_i' 在域 $\mathbf{K}(U_i,Y_{i-1})$ 中是不可约的且系数 $f_{ij}'(j=0,1,\cdots,d_i)$ 在 $\mathbf{K}[U_i]$ 中没有公因子.

注释 3.1.21　此后，扩张点的*定义多项式*等概念，按照扩张点的相应的表示类型，要么指 (3.1.1) 中的多项式 E_i, 要么指 (3.1.2) 中的 E_i'.

注释 3.1.22　如果 Ξ 是 $\mathbf{K}^n$ 中的一个普通点，则相应的定义多项式集为空，且 $\mathbf{K}(\Xi)=\mathbf{K}$.

<u>共轭扩张点</u>

定义 3.1.23　$\mathbf{K}^n$ 中有相同自由坐标和相同定义多项式集或相同定义方程组的扩张点称为 $\mathbf{K}^n$ 中的*共轭扩张点*.

假设给定一个扩张点 $\Xi=(\xi_1,\cdots,\xi_n)$, 其定义多项式集为 (3.1.1) 中的 E_i 或 (3.1.2) 中的 E_i'. 令 $\mathbf{K}_0$ 为扩域 $\mathbf{K}(\Xi_{c_1-1})$. 设 $\xi_1^{(i_1)}(i_1=1,\cdots,d_1)$ 是 $E_1=0$ 在 $\mathbf{K}_0$ 的某个扩域中的所有零点. 现记 $\mathbf{K}_1^{(i_1)}$ 为将 X_{c_2-1} 中的所有超越元 u_j 和零点 $\xi_1^{(i_1)}$ 加到 $\mathbf{K}_0$ 中所得到的扩域. 对于任一 $i_1=1,\cdots,d_1$, 令 $E_2^{(i_1)}$ 是由 E_2 或 E_2' 得到的 $\mathbf{K}_1^{(i_1)}[x_{c_2}]$ 中的多项式，其系数 $f_{2j}^{(i_1)}$ 是通过在 f_{2j} 中用 η_i 替换 $x_i(i=1,\cdots,c_2-1)$ 得到的，其中 $\eta_i=\xi_i$, 若 $i\neq c_1$; $\eta_{c_1}=\xi_1^{(i_1)}$ 记 $E_2^{(i_1)}=0$ 的所有零点为 $\xi_2^{(i_1i_2)},i_2=1,\cdots,d_2$. 记 $\mathbf{K}_2^{(i_1i_2)}$ 为将所有的 $\xi_i(c_2<i<c_3)$ 和 $\xi_2^{(i_1i_2)}$ 加到 $\mathbf{K}_1^{(i_1)}$ 中所得到的扩域. 显然，这一过程可归纳地继续下去. 最后我们得到了一个扩域 $\mathbf{K}_r^{(i_1\cdots i_r)}$, 一组方程 $E_r^{(i_1\cdots i_{r-1})}=0$ 和这组方程的零点集 $\xi_r^{(i_1\cdots i_{r-1}i_r)},i_r=1,\cdots,d_r$. 于是如下命题是显然的:

命题 3.1.24 所有扩张点 $\Xi^{(i_1\cdots i_r)}=(\eta_1,\cdots,\eta_n)$ 组成的集合，构成了共轭扩张点的全体，Ξ 是其中之一，其中 $\eta_j=\xi_j$, 若 j 不等于任意 $c_i,\eta_{c_1}=\xi_1^{(i_1)},\eta_{c_2}=\xi_2^{(i_1i_2)}$ 等等如上所得. 此外，扩域 $\mathbf{K}_r^{(i_1\cdots i_r)}$ 是 $\Xi^{(i_1\cdots i_r)}$ 的定义域，且彼此以自然的方式同构.

例 3.1.25 设 t 是一个未定元，则 (t^2,t^3,t^4) 和 $(t^2,-t^3,t^4)$ 是 $\mathbf{K}^3$ 中的共轭扩张点，且有相同的第一个自由坐标 t^2 和相同的定义多项式:

$$E_1 = x_2^2 - x_1^3, \qquad E_2 = x_3 - x_1^2.$$

<u>扩张点的维数</u>

命题 3.1.26 设一个扩张点 $\Xi=(\xi_1,\cdots,\xi_n)$ 的定义多项式集为 (3.1.1) 或 (3.1.2), 则扩张点 Ξ 在 $\mathbf{K}$ 上的维数等于 $n-r$.

证明 设 Ξ 的定义多项式如 (3.1.1) 或 (3.1.2). 于是显然有 $n-r$ 个元 ξ_j, 在 $\mathbf{K}$ 上代数独立，其中 j 不等于任一 c_k, 且每个 ξ_{c_k} 与这 $n-r$ 个元代数相关. 因此

$$\mathrm{Dim}_{\mathbf{K}}(\Xi)=\mathrm{TrDeg}(\mathbf{K}(\Xi)/\mathbf{K})=n-r. \tag{3.1.3}$$

命题证毕. □

一些极端情况:

$r=n$: $\mathrm{Dim}_{\mathbf{K}}(\Xi)=0$.

$r=n$ 且所有的 $d_i=1$: Ξ 是 $\mathbf{K}^n$ 中的一个普通点.

$r=0$: $\mathrm{Dim}_{\mathbf{K}}(\Xi)=n$.

例 3.1.27 设 $\mathbf{K}=\mathbf{R}$, $\Xi=(-i,+i)$, $\Xi'=(+i,-i)$, 其中 $i=\sqrt{-1}$. 点 Ξ 和 Ξ' 是 $\mathbf{R}^2$ 中的共轭扩张点，它们有相同的定义多项式:

$$x_1^2 + 1, \ x_2 + x_1.$$

因此，$n=r=2$ 且 $\mathrm{Dim}_{\mathbf{R}}\,\Xi = \mathrm{Dim}_{\mathbf{R}}\,\Xi' = 0$.

例 3.1.28 设 $\Xi=(\frac{2*t}{1+t^2},\frac{1-t^2}{1+t^2})$, $\Xi'=(\frac{1-t^2}{1+t^2},\frac{2*t}{1+t^2})$, 其中 t 是一个未定元. 首先注意到 $\xi_1=\frac{2*t}{1+t^2}$ 和 $\xi_1'=\frac{1-t^2}{1+t^2}$ 在 $\mathbf{K}$ 上是超越的. 因为假设有一个多项式 $P\in\mathbf{K}[x]$ 使得 $P(\xi_1)=0$, 则设 $P=a_0*x^d+\cdots+a_d$, 其中 $a_i\in\mathbf{K}$. 在 $P(\xi_1)=0$ 中消去分母，我们得到一个如下形式的方程:

$$a_0*(2*t)^d+\cdots+a_d*(1+t^2)^d = 0.$$

在上面的方程中令 $t=0$, 我们得到 $a_d=0$. 消去非零因子 $2*t$, 我们有如下方程:

$$a_0*(2*t)^{d-1}+\cdots+a_{d-1}*(1+t^2)^{d-1} = 0.$$

再在上面方程中令 $t=0$, 我们得到 $a_{d-1}=0$. 消去非零因子 $2*t$, 继续做下去我们将得到, 对于所有的 i 有 $a_i=0$ 或 $P\equiv 0$. 因此 ξ_1 在 $\mathbf{K}$ 上是超越的. 类似地对 ξ_1' 也可证明它的超越性.

此时容易看出, Ξ 和 Ξ' 具有相同的单个的定义多项式 $x_2^2+x_1^2-1$, 因此有 $n=2, r=1$. 故 $\mathrm{Dim}_{\mathbf{K}}\ \Xi = \mathrm{Dim}_{\mathbf{K}}\ \Xi' = 1$.

扩张点的特定化

定义 3.1.29 $\mathbf{K}^n$ 中的一个扩张点 Ξ' 称为 $\mathbf{K}^n$ 中的扩张点 Ξ 在 $\mathbf{K}$ 上的特定化, 如果对于任一满足 $P(\Xi)=0$ 的多项式 $P\in\mathbf{K}[X]$, 都有 $P(\Xi')=0$.

记号 3.1.30 对于 $\mathbf{K}^n$ 中的扩张点 Ξ, Ξ', Ξ' 是 Ξ 在 $\mathbf{K}$ 上的特定化记作

$$\Xi \underset{\mathbf{K}}{\longrightarrow} \Xi'. \tag{3.1.4}$$

记号 3.1.31 $\mathbf{K}^n$ 中的扩张点 Ξ 在 $\mathbf{K}$ 上的所有特定化组成的集合记为 $\mathrm{Spec}_{\mathbf{K}}(\Xi)$.

命题 3.1.32 $\mathbf{K}$ 中的任意两个共轭扩张点互为彼此在 $\mathbf{K}$ 上的特定化.

证明 由定义可归纳证得. 也可参看 §3.6. □

特定化的例子

命题 3.1.33 设 $\xi_1,\cdots,\xi_n$ 是独立未定元, 则 $\mathbf{K}^n$ 中的任一扩张点 $\Xi'=(\xi_1',\cdots,\xi_n')$ 都是 $\Xi=(\xi_1,\cdots,\xi_n)$ 的一个特定化.

证明 考虑 $\mathbf{K}[X]$ 中的任一多项式 $P(X)$, 则

$$P(\Xi)=0 \implies P(X)\equiv 0 \implies P(\Xi')=0.$$

因此 (3.1.4) 得证. □

命题 3.1.34 设 $\Xi=(\xi_1,\cdots,\xi_n)$ 是 $\mathbf{K}^n$ 中的一个扩张点, 其中每个 ξ_i 都等于某个参数为 $U=(u_1,\cdots,u_d)$, 系数在 $\mathbf{K}$ 中的有理函数. 设 u_j' 为 $\mathbf{K}$ 的任一扩域 $\mathbf{K}'$ 中的值, 它使得当每个 u_j 被 u_j' 代替时, 每一 ξ_i 有定义明确的值 ξ_i', 则 $\Xi'=(\xi_1',\cdots,\xi_n')$ 是 Ξ 在 $\mathbf{K}$ 上的一个特定化.

证明 设 $\xi_i=\frac{p_i}{q_i}$, 其中 $p_i, q_i\in\mathbf{K}[U]$ 且互素. 由假设, 对每个 i 有 $q_i(U')\neq 0$, 这里 $U'=(u_1',\cdots,u_d')$. 对 $\mathbf{K}[X]$ 中的任一多项式 $P(X)$, 我们有

$$\begin{aligned} P(\Xi)=0 \quad &\implies P\left(\frac{p_1(U)}{q_1(U)},\cdots,\frac{p_n(U)}{q_n(U)}\right)=0 \\ &\implies P\left(\frac{p_1(U')}{q_1(U')},\cdots,\frac{p_n(U')}{q_n(U')}\right)=0 \\ &\implies P(\Xi')=0. \end{aligned}$$

因此 (3.1.4) 得证. □

下面的例子说明并不是每个特定化都如在命题 3.1.33 和 3.1.34 中那样只通过作替换就可以得到.

例 3.1.35 在 $\mathbf{K}^3$ 中, 点 $(0,0,1)$ 是扩张点 $\Xi = \left(\xi_1, \xi_2, \frac{\xi_2}{\xi_1}\right)$ 的一个特定化, 其中 ξ_1, ξ_2 是 $\mathbf{K}$ 上的独立未定元.

证明 考虑任一满足 $P(\Xi) = 0$ 的多项式 $P(x_1, x_2, x_3) \in \mathbf{K}[x_1, x_2, x_3]$, 则

$$P\left(x_1, x_2, \frac{x_2}{x_1}\right) = 0. \tag{3.1.5}$$

将 P 看作一个关于变量 x_3 的多项式. 用 $x_1 * x_3 - x_2$ 除以 P, 则存在多项式 $Q \in \mathbf{K}[x_1, x_2, x_3]$ 以及 $R \in \mathbf{K}[x_1, x_2]$, 使得

$$x_1^d * P(x_1, x_2, x_3) = (x_1 * x_3 - x_2) * Q + R. \tag{3.1.6}$$

在方程 (3.1.6) 中, 令 $x_3 = \frac{x_2}{x_1}$, 则有

$$R = x_1^d * P\left(x_1, x_2, \frac{x_2}{x_1}\right) = 0.$$

因此, (3.1.6) 变为

$$x_1^d * P(x_1, x_2, x_3) = (x_1 * x_3 - x_2) * Q.$$

于是有 x_1^d 整除 Q, $x_1 * x_3 - x_2$ 整除 P, 从而对某个多项式 $P'(x_1, x_2, x_3) \in \mathbf{K}[x_1, x_2, x_3]$, 我们有

$$P(x_1, x_2, x_3) = (x_1 * x_3 - x_2) * P'(x_1, x_2, x_3).$$

通过直接的代换有 $P(0, 0, 1) = 0$.

由此, 对任一满足 $P(\Xi) = 0$ 的多项式 $P \in \mathbf{K}[x_1, x_2, x_3]$, 也有 $P(0, 0, 1) = 0$. 因此

$$\left(\xi_1, \xi_2, \frac{\xi_2}{\xi_1}\right) \underset{\mathbf{K}}{\longrightarrow} (0, 0, 1)$$

得证. □

例 3.1.36 在 $\mathbf{K}^2$ 中, 对于未定元 t, 我们有

$$\left(\frac{2 * t}{1 + t^2}, \frac{1 - t^2}{1 + t^2}\right) \underset{\mathbf{K}}{\longrightarrow} (0, 1) \text{ 和 } (0, -1). \tag{3.1.7}$$

证明 考虑多项式 $P(x_1, x_2) \in \mathbf{K}[x_1, x_2]$, 它满足

$$P\left(\frac{2 * t}{1 + t^2}, \frac{1 - t^2}{1 + t^2}\right) = 0.$$

把 P 看作关于变量 x_1 的多项式. 用 $x_1^2+x_2^2-1$ 除以 P, 则存在多项式 $Q(x_1,x_2)\in\mathbf{K}[x_1,x_2]$ 以及 $R_1(x_2),R_2(x_2)\in\mathbf{K}[x_2]$, 满足下面关系:

$$P=(x_1^2+x_2^2-1)*Q+x_1*R_1+R_2.$$

在 P,Q,R_1,R_2 中, 用 $\frac{2*t}{1+t^2},\frac{1-t^2}{1+t^2}$ 代换 x_1,x_2 后, 我们得到一个如下形式的等式:

$$P\left(\frac{2*t}{1+t^2},\frac{1-t^2}{1+t^2}\right)=\frac{2*t}{1+t^2}*R_1\left(\frac{1-t^2}{1+t^2}\right)+R_2\left(\frac{1-t^2}{1+t^2}\right).$$

上面的等式左边为零, 从而右边也等于零. 考察其次数, 则有

$$R_1\left(\frac{1-t^2}{1+t^2}\right)=0,\quad R_2\left(\frac{1-t^2}{1+t^2}\right)=0.$$

在例 3.1.28 中, 我们已经证明了 $\frac{1-t^2}{1+t^2}$ 在 $\mathbf{K}$ 上是超越的, 从而 $R_1(x_2)\equiv 0, R_2(x_2)\equiv 0$. 因此,

$$P(x_1,x_2)=(x_1^2+x_2^2-1)*Q(x_1,x_2).$$

故 $P(0,1)=0$ 且 $P(0,-1)=0$. 由于 P 在 $\mathbf{K}[x_1,x_2]$ 中的选取是任意的, (3.1.7) 得证. □

注释 3.1.37　可以通过用 0 替代 t 直接看出 $(0,1)$ 是 $(\frac{2*t}{1+t^2},\frac{1-t^2}{1+t^2})$ 的一个特定化. 可是对于 $(0,-1)$, 我们不能用直接替代的方法来找它的特定化.

注释 3.1.38　在 (3.1.35) 和 (3.1.36) 中用到的方法是一种一般方法, 这种方法在后面几节的理论里将有重要的作用.

问题 S　给定 $\mathbf{K}^n$ 中的两个扩张点, 判定一个扩张点是否是另一个的特定化.

这个问题将在本章中的 3.6 节中得到解决.

<u>特定化下的维数</u>

命题 3.1.39　对 $\mathbf{K}^n$ 中的扩张点 $\Xi=(\xi_1,\cdots,\xi_n),\Xi'=(\xi_1',\cdots,\xi_n')$, 我们有

$$\Xi\underset{\mathbf{K}}{\longrightarrow}\Xi'\Longrightarrow \mathrm{Dim}_{\mathbf{K}}\,\Xi\ \geq\ \mathrm{Dim}_{\mathbf{K}}\,\Xi'. \tag{3.1.8}$$

证明　设 $\mathrm{Dim}_{\mathbf{K}}\,\Xi'=e$, 因而所有的 ξ_i' 中, 在 $\mathbf{K}$ 上代数独立的元素的最大个数为 e. 为简单起见, 我们假设这些独立元是最前面的 e 个 ξ_i', 即 $\xi_1',\cdots,\xi_e'$. 于是 ξ 中最前面 e 个, 即 $\xi_1,\cdots,\xi_e$ 在 $\mathbf{K}$ 上也是代数独立的. 因若不然, 则存在某个非零多项式 $P\in\mathbf{K}[X_e]$, 使得 $P(\Xi_e)=0$. 由于 Ξ' 是 Ξ 在 $\mathbf{K}$ 上的特定

化，于是 $P(\Xi'_e) = 0$, 从而 $\xi'_1, \cdots, \xi'_e$ 也是代数相关的，这与假设矛盾．因此，$\mathrm{Dim}_{\mathbf{K}}\ \Xi \geq e$. □

扩张点的本原元

定义 3.1.40 $\mathbf{K}^n$ 中的扩张点 Ξ 的 *本原元* 定义为 $\mathbf{K}$ 上的一个代数元 θ, 使得

$$\mathbf{K}(\theta) \equiv \mathbf{K}(\Xi).$$

命题 3.1.41 对 (3.1.1) 所给的 Ξ, 存在整数 $n_1, \cdots, n_r$, 使得 $\theta = n_1 * x_{c_1} + \cdots + n_r * x_{c_r}$ 是 Ξ 的一个本原元.

证明 参见经典教材 [VdW1] 或 [H-P1]. 它的纯粹的存在性证明可转变为构造性证明．在此省略. □

射影空间和射影点

考虑 *射影空间* 有时要比考虑仿射空间更方便．在此，我们不准备讨论细节，而仅仅介绍如下的一些记号：

记号 3.1.42 $A^n_{\mathbf{K}}(X)$ 是指仿射 n 维空间 $\mathbf{K}^n(X)$.

${}^hX := (x_0 : x_1 : \cdots : x_n)$, 其中并非所有的 $x_i = 0$.

$P^n_{\mathbf{K}}({}^hX)$ 是指带有齐次坐标 ${}^hX$ 的 $\mathbf{K}$ 上的 n 维射影空间.

定义 3.1.43 $x_0 = 1$ 的齐次坐标 ${}^hX$ 称作 X 的 *完备齐次坐标*；$P^n_{\mathbf{K}}({}^hX)$ 称作仿射空间 $A^n_{\mathbf{K}}(X)$ 的 *完备射影空间*；x_0 称为 $P^n_{\mathbf{K}}({}^hX)$ 在 *无限处的坐标*；对于 $A^n_{\mathbf{K}}(X)$ 中的一个扩张点 $X' = (x'_1, \cdots, x'_n)$, X' 的 *齐次化点* 是指在 $P^n_{\mathbf{K}}({}^hX)$ 中齐次的扩张点 ${}^hX' = (1 : x'_1 : \cdots, x'_n)$.

记号 3.1.44 对一个关于 X 的总次数为 d 的多项式 $P \in \mathbf{K}[X]$ 和 P 中的一个单项式 $M = x_1^{i_1} * \cdots * x_n^{i_n}$, 记 ${}^hM$ 为单项式 $x_0^{i_0} * M$, 这里 $i_0 = d - (i_1 + \cdots + i_n)$.

定义 3.1.45 对一个关于 X 的总次数为 d 的多项式 $P \in \mathbf{K}[X]$, 定义 P 的 *齐次化多项式* 为将 P 中的每一个单项式 M 用 ${}^hM$ 替换后所得到的齐次多项式.

自然地，我们可以在射影空间中定义 *扩张点* 和 *特定化* 的概念，这里我们不再阐述．这里很重要的一点是，在射影空间中有如下命题，而在仿射空间中没有类似的命题，例子可参见 [VdW2] 的第 107 页.

命题 3.1.46 (特定化 - 扩张定理) 设 ξ, ξ' 是 n 维射影空间 $P^n_{\mathbf{K}}({}^hX)$ 中的两个扩张点，η 是 m 维射影空间 $P^m_{\mathbf{K}}({}^hY)$ 中一个具有齐次坐标 ${}^hY = (y_0 : y_1 : \cdots : y_m)$ 的扩张点．若 ξ' 是 ξ 在 $\mathbf{K}$ 上的特定化，则这一特定化可在 $\mathbf{K}$ 上扩展为对子 $(\xi, \eta) \underset{\mathbf{K}}{\longrightarrow} (\xi', \eta')$, 其中 η' 是 $P^m_{\mathbf{K}}({}^hY)$ 中的一点.

§3.2 代数簇和零点集

<u>基本概念和符号</u>

记号 3.2.1 $\mathbf{\Omega}, \mathbf{\Omega}^*, \mathbf{K}, X=(x_1,\cdots,x_n), X_k=(x_1,\cdots,x_k), A_{\mathbf{K}}^n(X)$ 等记号与第一章第 3.1 节中相同.

定义 3.2.2 ($\mathbf{K}$ 上关于 X 的) *多项式* 是指 $\mathbf{K}[X]$ 中的多项式.

定义 3.2.3 ($\mathbf{K}$ 上关于 X 的)*多项式集* 是指 $\mathbf{K}[X]$ 中的多项式集.

约定 除非另作说明, 多项式集都是有限的.

定义 3.2.4 $\mathbf{K}^n$ 中满足 $P(\Xi)=0$ 的一个扩张点 Ξ 称作多项式 $P\in\mathbf{K}[X]$ 的一个 *零点*.

定义 3.2.5 多项式集 PS 中所有多项式的一个公共零点称作 $PS\subset\mathbf{K}[X]$ 的一个 *零点*.

定义 3.2.6 多项式集 PS 的所有零点组成的集合称作 $PS\subset\mathbf{K}[X]$ 的 *零点集*.

记号 3.2.7 对于 $PS\subset\mathbf{K}[X]$, 用 $\mathrm{Zero}(PS)$ 记 PS 的零点集.

定义 3.2.8 两个多项式集 $PS_1, PS_2\subset\mathbf{K}[X]$ 称作是 *0- 等价* 的, 如果 $\mathrm{Zero}(PS_1)=\mathrm{Zero}(PS_2)$.

记号 3.2.9 PS_1, PS_2 是0-等价的记作 $PS_1\sim_0 PS_2$.

记号 3.2.10 对于多项式 $PS, PS_1, PS_2\subset\mathbf{K}[X]$, 多项式 $G\in\mathbf{K}[X]$, $\mathbf{K}$ 的扩域 $\mathbf{F}$ 和 $\mathbf{K}^n$ 的子集 D, 由定义可记:

$$\left.\begin{array}{l}PS_1\times PS_2:=\{P_{1i}*P_{2j}\mid P_{1i}\in PS_1, P_{2j}\in PS_2\},\\ \mathrm{Zero}(PS/G):=\mathrm{Zero}(PS)\setminus\mathrm{Zero}(G),\\ \mathrm{Zero}_{\mathbf{F}}(PS/G):=\mathrm{Zero}(PS/G)\cap\mathbf{F}^n,\\ D\mathrm{Zero}(PS/G):=\mathrm{Zero}(PS/G)\cap D.\end{array}\right\}\qquad(3.2.9)$$

注释 3.2.11 除非另作说明, 下文中的基域 $\mathbf{K}$ 被当作已经指定并确定了, 所以不出现在记号中. 在 $(3.2.9)_3$ 中, $\mathbf{F}^n$ 中的点是指 $\mathbf{K}^n$ 中坐标在 $\mathbf{F}$ 中的点的全体, $(3.2.9)_4$ 中的 D 的意义也类似.

记号 3.2.12 对于多项式 $P_1, P_2\in\mathbf{K}[X]$ 和多项式集 $PS=\{A_1,\cdots,A_m\}\subset\mathbf{K}[X]$,

$$P_1\equiv P_2 \bmod_{\mathbf{K}} PS$$

是指存在多项式 $Q_1,\cdots,Q_m\subset\mathbf{K}[X]$, 使得

$$P_1-P_2=\sum_i Q_i*A_i.$$

注释 3.2.13 在本书中，我们用 + 而不用 ∪ 表示集合的并，但保留符号 \ 作为差集的运算符.

作为零点集的代数簇

定义 3.2.14 $\mathbf{K}^n$ 或 $A_{\mathbf{K}}^n(X)$ 中 (或在 $A_{\mathbf{K}}^n(X)$ 中的 $\mathbf{K}$ 上) 的一个 仿射代数簇, 简称 簇, 定义为 $\mathbf{K}[X]$ 中某个多项式集的零点集.

定义 3.2.15 对簇 $V = \mathrm{Zero}(PS)$, 称 PS 为 V 的一组 基.

定义 3.2.16 给定簇 $V = \mathrm{Zero}(PS)$, 其基 PS 是 $\mathbf{K}[X]$ 中的一个多项式集， PS 的一个零点称作 簇 V 的或 V 上的一点.

定义 3.2.17 给定簇 $V = \mathrm{Zero}(PS)$, 其中 PS 是 $\mathbf{K}[X]$ 中的一个多项式集，多项式 $G \in \mathbf{K}[X]$, 在 V 上 $G = 0$ 是指 $\mathrm{Zero}(PS) \subset \mathrm{Zero}(G)$, 或 PS 的任一零点都是 G 的一个零点.

记号 3.2.18 对簇 V 和多项式 G, 若在 V 上 $G = 0$ 或 $V \subset \mathrm{Zero}(G)$, 则记 $G = 0|V$.

简单性质

命题 3.2.19 设 PS, PS_1, PS_2 是 $\mathbf{K}[X]$ 中的多项式集， F_1, F_2, G, G_1, G_2 是 $\mathbf{K}[X]$ 中的多项式，则

$$\left.\begin{array}{l}
PS_1 \subset PS_2 \Longrightarrow \mathrm{Zero}(PS_2) \subset \mathrm{Zero}(PS_1).\\
\mathrm{Zero}(1) = \emptyset.\\
\mathrm{Zero}(0) = \mathrm{Zero}(\emptyset) = \mathbf{\Omega}^{*n}.\\
\mathrm{Zero}(PS/1) = \mathrm{Zero}(PS).\\
\mathrm{Zero}(PS/0) = \emptyset.\\
\mathrm{Zero}(PS/G_1 * G_2) = \mathrm{Zero}(PS/G_1) \cap \mathrm{Zero}(PS/G_2).\\
\mathrm{Zero}(PS) = \mathrm{Zero}(PS/G) + \mathrm{Zero}(PS + \{G\}).\\
\mathrm{Zero}(PS_1 + PS_2\ /\ G) = \mathrm{Zero}(PS_1/G) \cap \mathrm{Zero}(PS_2/G).\\
\mathrm{Zero}(PS + \{F_1 * F_2\}) = \mathrm{Zero}(PS + \{F_1\}) + \mathrm{Zero}(PS + \{F_2\}).\\
\mathrm{Zero}(PS_1) + \mathrm{Zero}(PS_2) = \mathrm{Zero}(PS_1 \times PS_2).
\end{array}\right\} \quad (3.2.10)$$

证明 作为例子，我们证明 (3.2.10) 中的最后一个等式. 若 Ξ 是该等式左边 L 中的一个点，则它是 $\mathrm{Zero}(PS_1)$ 或 $\mathrm{Zero}(PS_2)$ 中的一个零点. 若它是 $\mathrm{Zero}(PS_1)$ 中的一个零点，则它是 PS_1 中所有多项式 P_i 的一个零点，因而也是 $PS_1 \times PS_2$ 中所有多项式的零点，或者说 L 包含在该等式的右边 R 中. 类似地， $\mathrm{Zero}(PS_2)$ 中的零点也如此，因此 $L \subset R$. 现考虑 R 中的任一点，它也是所有形如 $P_{1i} * P_{2j}$ 的多项式的零点，其中 $P_{1i} \in PS_1$, $P_{2j} \in PS_2$,. 假设这

一点不是 Zero(PS_1) 中的零点，它必不是 PS_1 中某一多项式 P_{1i_1} 的零点. 由于它是所有形如 $P_{1i_1} * P_{2j}$ 的多项式的零点，其中 $P_{2j} \in PS_2$, 从而它必是所有 P_{2j} 的一个零点或者说它是 Zero(PS_2) 中的一个零点. 类似地，如果这个点不是 Zero(PS_2) 中的零点，它必是 Zero(PS_1) 中的一个零点. 不管怎样，这个点都在 L 中. 因此 $R \subset L$, 故 $L = R$. □

约定 由于我们感兴趣的是多项式集的零点而不是多项式集本身，并且多项式集中有 0 多项式不影响它的零点集，所以，除非另作说明，一般我们都假设 0 多项式不出现在任一个多项式集中.

一些例子

例 3.2.20 对 $P = x_1^2 + x_2^2 - 1 \in \mathbf{K}[x_1, x_2]$, (1,0), (0,1), $(\frac{2*t}{1+t^2}, \frac{1-t^2}{1+t^2})$ 都在 Zero(P) 中，其中 t 为未定元. 设 ξ_1 是未定元，ξ_2 是 $x_2^2 - 1 + \xi_1^2 = 0$ 在 $\mathbf{K}(\xi_1)$ 的某一扩域中的任一解，则 (ξ_1, ξ_2) 也是 Zero(P) 的一个零点.

例 3.2.21 假设在一个适当选取的坐标系中，一个几何定理 T 的假设由 $HYP = 0$ 给出，其中 $HYP \subset \mathbf{K}[X]$. 这样多项式集 HYP 的任一零点恰为扩张空间 $\mathbf{\Omega}^{*n}$ 中一个验证定理 T 的假设的几何图型. 如果这个定理的结论由 $CONC = 0$ 给出，其中 $CONC \in \mathbf{K}[X]$, 则定理为真，如果在簇 Zero(HYP) 上 $CONC = 0$ 或 Zero(HYP) $\subset$ Zero($CONC$). 一般而言，这一条件只在某些非退化条件 $ND_i \neq 0$ 成立时才满足，这里的 ND_i 是 $\mathbf{K}[X]$ 中的多项式. 于是定理的成立就化简为如下形式:

$$\mathrm{Zero}(HYP \ / \ \Pi_i \ ND_i) \subset \mathrm{Zero}(CONC). \qquad (3.2.11)$$

证明这样一个定理实际上就归结为找到非退化条件 $ND_i \neq 0$ 使得上面的包含关系 (3.2.11) 成立. 这就是我们的机械化几何定理证明的基本原理. 想要了解更多的细节可参见第一部分的第七章，该章主要研究机械化几何定理的证明.

例 3.2.22 设 $n = 3$, $\mathbf{K} = \mathbf{Q}$, n 为任一正整数，且 $P_n = x_1^n + x_2^n - x_3^n$, 于是费马最后定理相当于

$$\mathrm{Zero}_{\mathbf{Q}}(P_n / x_1 * x_2 * x_3) = \emptyset, \quad 当\ n > 2\ 时.$$

另一方面，§2.3 中的勾股有理三边公式 (2.3.19) 指出，当 $n = 2$ 时，

$$\mathrm{Zero}_{\mathbf{Q}}(P_2) = \{(a * (m^2 - n^2), 2 * a * m * n, a * (m^2 + n^2)) \mid a \in \mathbf{Q}, m, n \in \mathbf{Z}\}.$$

例 3.2.23 给定多项式 $P_1, P_2 \in \mathbf{K}[x_1]$, 且

$$P_i = a_{i0} * x_1^{d_i} + \cdots + a_{ij} * x_1^{d_i - j} + \cdots + a_{id_i}, \ a_{ij} \in \mathbf{K}, \qquad i = 1, 2.$$

设 R 为 P_1, P_2 关于 x_1 的结式. 若 a_{10}, a_{20} 不全为零, 则 P_1, P_2 有公共零点当且仅当 $R=0$. 于是

$$\mathrm{Zero}(P_1, P_2) \neq \emptyset \iff R = 0(\ a_{10}, a_{20} \text{ 不全为零}). \tag{3.2.12}$$

下文中, 除非另作说明, 所有的多项式和多项式集都在 $\mathbf{K}[X]$ 中, 所有的簇都在 $\mathbf{K}^n$ 中且非空.

<u>不可约代数簇</u>

定义 3.2.24 代数簇 $V_1 = \mathrm{Zero}(PS_1)$ 称作代数簇 $V_2 = \mathrm{Zero}(PS_2)$ 的 *子簇*, 如果 $V_1 \subset V_2$. 称 V_1 是 V_2 的 *真子簇*, 如果 $V_1 \subset V_2$ 且 $V_1 \neq V_2$.

定义 3.2.25 $\mathbf{K}^n$ 中的代数簇 $V = \mathrm{Zero}(PS)$ 称作在 $\mathbf{K}$ 上 *不可约*, 如果 V 不能写成 $\mathbf{K}^n$ 中的两个真子簇的并. V 称作是 *可约的*, 如果 V 不是不可约的.

注释 3.2.26 簇的不可约性依赖于基域 $\mathbf{K}$. 例如, 簇 $V = \mathrm{Zero}(x_1^2+1)$ 在域 $\mathbf{K}=\mathbf{R}$ 上是不可约的, 但在 $\mathbf{K}=\mathbf{C}$ 上是可约的, 因为 $V = \mathrm{Zero}(x_1+i) + \mathrm{Zero}(x_1-i)$, 其中 $i=\sqrt{-1}$.

<u>一些简单命题</u>

命题 3.2.27 若 $V_1 = \mathrm{Zero}(PS_1)$ 是 $V = \mathrm{Zero}(PS)$ 的一个真子簇, 则存在多项式 $P_1 \in PS_1$, 使得 $P_1 \neq 0|V$.

证明 假若对所有的多项式 $P_1 \in PS_1$, 都有 $P_1 = 0|V$ 或 $\mathrm{Zero}(PS) \subset \mathrm{Zero}(P_1)$, 则 $\mathrm{Zero}(PS) \subset \mathrm{Zero}(PS_1)$. 于是 $\mathrm{Zero}(PS_1) = \mathrm{Zero}(PS)$, 矛盾于假设. □

命题 3.2.28 两个簇的交和并也是簇.

证明 直接由 $(3.2.10)_8$ 和 $(3.2.10)_{10}$ 得出. □

命题 3.2.29 若一个不可约簇 V 包含在两个簇 V_1 和 V_2 的并中, 则 V 完全包含在 V_1 中或完全包含在 V_2 中.

证明 由假设有 $V \subset V_1 + V_2$, 因而

$$V = V \cap V_1 + V \cap V_2.$$

由于 V 是不可约的, 从而 $V \cap V_1$ 作为 V 的一个子簇, 或等于 V 或是空集. 类似地, $V \cap V_2$ 或等于 V 或是空集. 因此, 非空集 V 或者等于 $V \cap V_1$ 或者等于 $V \cap V_2$. 若 $V = V \cap V_1$, 则 $V \subset V_1$. 若 $V = V \cap V_2$, 则 $V \subset V_2$. □

命题 3.2.30 簇中的点在 $\mathbf{K}$ 上的任一特定化也是这个簇的点.

证明 设 Ξ 是簇 $V = \mathrm{Zero}(PS)$ 中的点, 且使得对于任一多项式 $P \in PS$ 都有 $P(\Xi) = 0$. 若 Ξ' 是 Ξ 在 $\mathbf{K}$ 上的一个特定化, 则对所有的 $P \in PS$ 也有

$P(\Xi')=0$, 从而 Ξ' 是 V 中的一点. □

不可约性的判定

定理 3.2.31 (判定定理 1)　$\mathbf{K}^n$ 中的一个代数簇 $\mathrm{Zero}(PS)$ 在 $\mathbf{K}$ 上不可约当且仅当若存在一对多项式 $P_1,P_2\in\mathbf{K}[X]$ 使得 $\mathrm{Zero}(PS)\subset\mathrm{Zero}(P_1*P_2)$, 则有 $\mathrm{Zero}(PS)\subset\mathrm{Zero}(P_1)$, 或 $\mathrm{Zero}(PS)\subset\mathrm{Zero}(P_2)$. 换言之, 由 $P_1*P_2=0|\mathrm{Zero}(PS)$ 可推出 $P_1=0|\mathrm{Zero}(PS)$ 或 $P_2=0|\mathrm{Zero}(PS)$.

证明　首先假设 $\mathrm{Zero}(PS)$ 是不可约的, 且 $P_1*P_2=0|\mathrm{Zero}(PS)$. 现由 $(3.2.10)_9$,

$$\mathrm{Zero}(PS)\subset\mathrm{Zero}(P_1*P_2)\Longrightarrow\mathrm{Zero}(PS)\subset\mathrm{Zero}(P_1)+\mathrm{Zero}(P_2).$$

由于 $\mathrm{Zero}(PS)$ 是不可约的, 从而由命题 3.2.29 有 $\mathrm{Zero}(PS)\subset\mathrm{Zero}(P_1)$ 或 $\mathrm{Zero}(PS)\subset\mathrm{Zero}(P_2)$. 因此, 最后的条件是 $\mathrm{Zero}(PS)$ 不可约的必要条件.

反过来, 设 $\mathrm{Zero}(PS)$ 不是不可约的, 因而 $\mathrm{Zero}(PS)$ 是两个真子簇 $V_1=\mathrm{Zero}(PS_1)$ 和 $V_2=\mathrm{Zero}(PS_2)$ 的并. 于是由命题 3.2.19, 存在多项式 $P_1\in PS_1$, 使得 $P_1\neq 0|\mathrm{Zero}(PS)$; 存在多项式 $P_2\in PS_2$, 使得 $P_2\neq 0|\mathrm{Zero}(PS)$. 现在有

$$P_1\in PS_1\Longrightarrow P_1=0|V_1\Longrightarrow P_1*P_2=0|V_1.$$

类似地,

$$P_1*P_2=0|V_2.$$

因此

$$P_1*P_2=0\mid\mathrm{Zero}(PS_1)+\mathrm{Zero}(PS_2)=V_1+V_2=\mathrm{Zero}(PS),$$

从而最后的条件不满足. 故最后的条件也是 $\mathrm{Zero}(PS)$ 不可约的充分条件. □

定理 3.2.32 (判定定理 2)　$\mathbf{K}^n$ 中的一个代数簇 $V=\mathrm{Zero}(PS)$ 在 $\mathbf{K}$ 上不可约当且仅当 V 上存在 $\mathbf{K}^n$ 中的一个扩张点 Ξ, 使得 V 的所有点都是 Ξ 在 $\mathbf{K}$ 上的特定化. 换言之, 当且仅当

$$\mathrm{Zero}(PS)=\mathrm{Spec}_{\mathbf{K}}(\Xi).\tag{3.2.13}$$

证明　首先假设存在这样一点 Ξ 满足 (3.2.13). 考虑 $\mathbf{K}[X]$ 中满足 $P_1*P_2=0|V$ 的任意两个多项式 P_1,P_2. 特别地, 我们有 $(P_1*P_2)(\Xi)=0$, 因而 $P_1(\Xi)=0$ 或 $P_2(\Xi)=0$. 由 (3.2.13), V 的任一点 Ξ' 都是 Ξ 在 $\mathbf{K}$ 上的特定化, 因此, 对所有的 $\Xi'\in V$ 有 $P_1(\Xi')=0$, 或者对所有的 $\Xi'\in V$ 有 $P_2(\Xi')=0$. 这表明 $P_1=0|V$ 或 $P_2=0|V$. 由定理 3.2.31, V 是不可约的.

现在假设 V 是不可约的. 为保证存在一个满足 (3.2.13) 的点 Ξ, 我们对 $\mathbf{K}[X]$ 中的多项式引入一个等价关系 $\sim$, 使得对于 $P_1,P_2\in\mathbf{K}[X],P_1\sim P_2$ 当

且仅当 $P_1 - P_2 = 0|V$. 我们记 $[P]$ 为多项式 P 的等价类. 定义 $[P_1]+[P_2]=[P_1+P_2]$,$[P_1]*[P_2]=[P_1*P_2]$. 容易看出这一定义是合理的, 且所有这样的等价类形成一个环 $\mathbf{A}$. 若对于任一 $k\in\mathbf{K}$, 把 $[k]$ 和 k 看成是等同的, 则 $\mathbf{K}$ 是 $\mathbf{A}$ 的一个子环. 此外, 由 $[P_1]*[P_2]=0$ 有 $[P_1*P_2]=[0]$ 或 $P_1*P_2=0|V$. 由于 V 是不可约的, 从而 $P_1=0|V$ 或 $P_2=0|V$, 即 $[P_1]=[0]=0$ 或 $[P_2]=[0]=0$. 因此, 上述环 $\mathbf{A}$ 是一个整环, 从而有商域 $\mathbf{A}^*$. 显然, $\mathbf{A}^*$ 是 $\mathbf{K}$ 的一个扩域. 现考虑 $\mathbf{A}^{*n}$ 中的扩张点 $\Xi=([x_1],\cdots,[x_n])$. 对任一多项式 $P\in PS$, 我们有 $P(\Xi)=[P(X)]=0|\mathrm{Zero}(PS)$ 或 $\Xi\in V$. 由命题 3.2.30 知 $\mathrm{Spec}_{\mathbf{K}}(\Xi)\subset V$. 现考虑 V 中的任一点 $\Xi'\in V$. 对任一 $P\in\mathbf{K}[X]$ 且 $P(\Xi)=0$, 我们有 $[P(X)]=0$ 或 $P(X)=0|V$, 因此 $P(\Xi')=0$. 由此有 Ξ' 是 Ξ 在 $\mathbf{K}$ 上的特定化, 从而 $V\subset\mathrm{Spec}_{\mathbf{K}}(\Xi)$. 因此 $V=\mathrm{Spec}_{\mathbf{K}}(\Xi)$, 即点 Ξ 满足上述 (3.2.13). □

<u>母点的概念</u>

定义 3.2.33 $\mathbf{K}^n$ 中任一满足 (3.2.13) 的扩张点 Ξ 称作不可约簇 $\mathrm{Zero}(PS)$ 的一个 *母点*.

由上面的定义, 定理 3.2.32 可改述为

定理 3.2.34 (基本定理) $\mathbf{K}^n$ 中的一个代数簇在 $\mathbf{K}$ 上不可约当且仅当它有一个 $\mathbf{K}$ 上的母点.

一个不可约簇的母点不是唯一的. 然而, 由它的定义可得到定理 3.2.34 的如下推论:

定理 3.2.35 对 $\mathbf{K}^n$ 中的一个不可约代数簇, 任意两个母点在 $\mathbf{K}$ 上互为特定化.

<u>不可约簇的维数</u>

由定理 3.2.35 和命题 3.1.39, 我们可知如下定义是合理的:

定义 3.2.36 $\mathbf{K}^n$ 中一个不可约代数簇 V 的 *维数* 定义为该簇的任一个母点在 $\mathbf{K}$ 上的维数.

记号 3.2.37 一个不可约簇 V 在 $\mathbf{K}$ 上的维数记为 $\mathrm{Dim}_{\mathbf{K}}\,V$.

定理 3.2.38 若 $V'=\mathrm{Zero}(PS')$ 是一个不可约簇 $V=\mathrm{Zero}(PS)$ 的不可约真子簇, 则

$$\mathrm{Dim}_{\mathbf{K}}V' < \mathrm{Dim}_{\mathbf{K}}V. \tag{3.2.14}$$

证明 设 Ξ 和 Ξ' 分别是 V 和 V' 的母点. 由 $V'\subset V$ 知, Ξ' 是 Ξ 的一个特定化. 于是由命题 3.1.39 有

$$\mathrm{Dim}_{\mathbf{K}}\,V' = \mathrm{Dim}_{\mathbf{K}}\,\Xi' \le \mathrm{Dim}_{\mathbf{K}}\,\Xi = \mathrm{Dim}_{\mathbf{K}}\,V.$$

假若 V 和 V' 有相同的维数 e. 设 $\Xi' = (\xi_1', \cdots, \xi_n')$, 其中 $\xi_{i_1}', \cdots, \xi_{i_e}'$ 是代数独立的, 而其他 ξ_i' 与它们代数相关, 则对于 $\Xi = (\xi_1, \cdots, \xi_n)$, $\xi_{i_1}, \cdots, \xi_{i_e}$ 也是代数独立的, 而其他 ξ_i 与这些 ξ_i 代数相关. 由命题 3.2.27 和假设, 存在一个多项式 $P \in \mathbf{K}[X]$, 使得 $P = 0|V'$ 但 $P \neq 0|V$. 由此有 $P(\Xi') = 0$ 但 $P(\Xi) \neq 0$. 显然, $P(\Xi)$ 是与 $\xi_{i_1}, \cdots, \xi_{i_e}$ 代数相关的, 从而有多项式

$$F = a_0 * x^s + \cdots + a_s,$$

其中 $a_i \in \mathbf{K}[x_{i_1}, \cdots, x_{i_e}]$, 且 $a_0 \neq 0, a_s \neq 0$, 使得当每个 x_{i_k} 被 ξ_{i_k} 代替时, a_j 的值是 α_j. 于是, $x = P(\Xi)$ 满足方程

$$\alpha_0 * x^s + \cdots + \alpha_s = 0.$$

显然 $\alpha_0 \neq 0$, 因为 $\xi_{i_1}, \cdots, \xi_{i_e}$ 是代数独立的.

现设当每个 x_{i_k} 由 ξ_{i_k}' 代替时, a_j 的值是 α_j'. 由于 Ξ' 是 Ξ 的一个特定化, 我们知 $P(\Xi')$ 满足方程

$$\alpha_0' * x^s + \cdots + \alpha_s' = 0.$$

如前有 $\alpha_0' \neq 0$. 另一方面由 $P(\Xi') = 0$ 知 0 满足如上方程, 故 $\alpha_s' = 0$. 由于 $a_s \neq 0$, 从而 $\xi_{i_1}', \cdots, \xi_{i_e}'$ 是代数相关的, 矛盾！因此, 维数相等的假设不成立, 于是有 (3.2.14). □

<u>特殊维数的不可约簇</u>

定理 3.2.39 簇 Zero($\emptyset$) 或 Zero(0) 是 $\mathbf{K}^n$ 中唯一的维数为 n 的不可约簇, 它具有母点 $X = (x_1, \cdots, x_n)$, 其中 $x_1, \cdots, x_n$ 为独立未定元.

证明 直接由 3.1 节的命题 3.1.34 得到. □

定理 3.2.40 $\mathbf{K}^n$ 中唯一的维数为 $n-1$ 的不可约簇具有形式 Zero(P), 其中 P 是 $\mathbf{K}[X]$ 中的某一非零不可约多项式.

证明 首先考虑形如 $V = \text{Zero}(P)$ 的簇, 其中 $P \in \mathbf{K}[X]$ 是不可约的. 设 x_c 出现在 P 中, 但对于所有 $i > c$, x_i 都不出现在 P 中, 因而 $P \in \mathbf{K}[X_c]$. 令 $\Xi = (x_1, \cdots, x_{c-1}, \xi_c, x_{c+1}, \cdots, x_n)$, 其中 ξ_c 是 $P(X) = 0$ 的一个解. 考虑任一满足 $F(\Xi) = 0$ 的多项式 $F \in \mathbf{K}[X]$ 和任一 $\Xi' = (\xi_1', \cdots, \xi_n') \in \text{Zero}(P)$. 由于 P 不可约, 从而 P 可整除 F, 因此 $F(\Xi') = 0$. 于是, Ξ' 是 Ξ 在 $\mathbf{K}$ 上的特定化, 从而 Ξ 是 V 的一个母点. 故 V 在 $\mathbf{K}$ 上不可约. 显然, $\text{Dim}_\mathbf{K} V = \text{Dim}_\mathbf{K} \Xi = n-1$.

反过来, 设 $V = \text{Zero}(PS)$ 是 $\mathbf{K}^n$ 中一个维数为 $n-1$ 的不可约簇. 从 PS 中任取多项式 P, 把 PS 写为形式 $PS = PS' + \{P\}$. 设 $P = P_1 * \cdots * P_r$, 其中

P_i 都是 $\mathbf{K}[X]$ 中的不可约多项式. 于是有

$$\begin{aligned} V &= \text{Zero}(PS' + \{P\}) = \text{Zero}(PS' + \{P_1 * \cdots P_r\}) \\ &= \text{Zero}(PS' + \{P_1\}) + \cdots + \text{Zero}(PS' + \{P_r\}). \end{aligned}$$

由于 V 是不可约的, 由命题 3.2.29 有

$$V \subset \text{Zero}(PS' + \{P_i\}) \subset \text{Zero}(P_i),$$

对于某个 i. 由前一部分知, $\text{Zero}(P_i)$ 是不可约的且 $\text{Dim}_{\mathbf{K}}\ \text{Zero}(P_i) = n-1$. 由假设, 不可约簇 V 和 $\text{Zero}(P_i)$ 在 $\mathbf{K}$ 上有相同的维数. 于是, 由定理 3.2.38 有 $V = \text{Zero}(P_i)$. □

定理 3.2.41 $\mathbf{K}^n$ 中任一维数为 0 的不可约簇 V 是 $\mathbf{K}$ 上有限个共轭点组成的集合.

证明 设 $\Xi = (\xi_1, \cdots, \xi_n)$ 是不可约簇 V 的一个母点, 则 $\text{Dim}_{\mathbf{K}}\ \Xi = 0$, 从而 Ξ 的定义多项式集有形式

$$\begin{aligned} P_1 &= x_1^{d_1} + f_{11} * x_1^{d_1-1} + \cdots + f_{1d_1}, \\ P_2 &= x_2^{d_2} + f_{21} * x_2^{d_2-1} + \cdots + f_{2d_2}, \\ &\cdots\cdots\cdots\cdots \\ P_n &= x_n^{d_n} + f_{n1} * x_n^{d_n-1} + \cdots + f_{nd_n}, \end{aligned}$$

其中 $f_{ij} \in \mathbf{K}(X_{i-1})$. 由于 Ξ 是所有这些多项式 P_i 的一个零点, 且 V 的任一点 $\Xi' = (\xi'_1, \cdots, \xi'_n)$ 都是 Ξ 在 $\mathbf{K}$ 上的特定化, 从而也是所有这些多项式的一个零点. 反过来, 由 §3.1 的命题 3.1.32, 这些方程的任一解 Ξ' 都是 Ξ 在 $\mathbf{K}$ 上的一个特定化, 因此 Ξ' 是 V 的一个点. 由此知簇 $V = \text{Zero}(PS)$ 由这样的 Ξ' 组成, 其中 $PS = \{P_1, \cdots, P_n\}$. 这样的点 Ξ' 共有 $\Pi_i\ d_i$ 个, 且是相互共轭的. 定理证毕. □

<u>母点的例子</u>

例 3.2.42 $\mathbf{K}^3(x_1, x_2, x_3)$ 中的代数簇 $V = \text{Zero}(x_1 * x_3 - x_2)$ 在 $\mathbf{K}$ 中不可约, 其母点为 $(x_1, x_2, \frac{x_2}{x_1})$, 其中 x_1, x_2 是独立未定元. 我们有 $\text{Dim}_{\mathbf{K}}\ V = 2$. 如果 V 被看作 $\mathbf{K}^n(x_1, \cdots, x_n)$ 中的一个代数簇, 其中 $n > 3$, 则 V 的维数 $\text{Dim}_{\mathbf{K}}\ V = n-1$, 且有一个母点 $(x_1, x_2, \frac{x_2}{x_1}, x_4, \cdots, x_n)$, 其中 $x_1, x_2, x_4, \cdots, x_n$ 是独立未定元. 参见例 3.1.35.

例 3.2.43 簇 $V = \text{Zero}(x_2^2 + x_1^2 - 1)$ 在 $\mathbf{K}^2(x_1, x_2)$ 中是不可约的, 其母点为 $(\frac{2*t}{1+t^2}, \frac{1-t^2}{1+t^2}), (\frac{1-t^2}{1+t^2}, \frac{2*t}{1+t^2})$, 或更一般地, 为 (x_1, ξ_2), 其定义多项式集为 $\{x_2^2 + x_1^2 - 1\}$, 这里的 t 和 x_1 都是未定元. 参见例 3.1.28.

簇的不可约分解

定理 3.2.44　一个真子簇序列

$$V_1 \supset V_2 \supset \cdots$$

将在有限步终止.

证明　设 $V_i = \mathrm{Zero}(PS_i)$, 且 PS 是所有这些 PS_i 的并. 由 Hilbert 有限基定理, 存在一个有限集合 $FS \subset PS$, 使得 $\mathrm{Zero}(FS) = \mathrm{Zero}(PS)$. 若 FS 包含在 PS_k 中, 则序列将在第 k 步终止. □

定理 3.2.45　簇 V 可分解为 V 的有限个不可约真子簇的并.

证明　假若定理不成立, V 是不具有如下性质 (P) 的簇:

(P)　簇可分解为有限个不可约真子簇的并.

不具有性质 (P) 的簇 V 应该不是不可约的. 设 $V = V_1 + V_1'$, 其中 V_1, V_1' 都是 V 的真子簇. 于是 V_1, V_1' 中至少有一个, 假设为 V_1, 不具有性质 (P). 同理, V_1 是可约的, 且有形式 $V_1 = V_2 + V_2'$, 其中 V_2, V_2' 都是 V_1 的真子簇. 由于 V_1 不具有性质 (P), 从而 V_2, V_2' 中至少有一个, 假设为 V_2, 也不具有性质 (P). 如此继续下去, 则得到一个无限真子簇序列 $V_1 \supset V_2 \supset \cdots$, 这与定理 3.2.44 矛盾. 因此, 不存在不具有性质 (P) 的簇, 定理证毕. □

定义 3.2.46　簇 V 的如下形式的子簇 V_i 分解:

$$V = V_1 + \cdots + V_m, \tag{3.2.15}$$

称作 V 的一个不可约分解, 如果每个 V_i 都是 V 的一个不可约真子簇. 分解 (3.2.15) 称作是不可缩的, 如果分解式中的每个 V_i 都不包含在其他 V_j 的并中.

定理 3.2.45 可以加强为如下形式:

定理 3.2.47 (簇分解定理)　任一簇 V 都有一个不可缩的不可约真子簇分解.

证明　由定理 3.2.45, 任一簇 V 都有一个形如 (3.2.15) 的不可约分解. 如果某个 V_i 包含在其他 V_j 的并中, 就从并中去掉这个 V_i. 如此继续下去, 直到得到某一不可缩分解. □

定理 3.2.48　不考虑子簇的顺序, 一个簇的不可缩不可约分解是唯一的.

证明　设 (3.2.15) 和下面的 (3.2.16) 是同一簇 V 的两个不可缩不可约分解:

$$V = V_1' + \cdots + V_{m'}'. \tag{3.2.16}$$

不可约子簇 V_1' 包含在 V 中，其中 V 有分解 (3.2.15). 由命题 3.2.29, V_1' 包含在某个 V_i, 比如说 V_{i_1} 中. 同样地，V_{i_1}, 包含在具有分解 (3.2.16) 的 V 中，从而包含在某个 V_i', 比如 V_k' 中. 于是有 $V_1' \subset V_k'$. 由于分解 (3.2.16) 是不可缩的，从而有 $V_1' = V_k'$. 又由 $V_1' \subset V_{i_1} \subset V_k'$ 知 $V_1' = V_{i_1}$. 用同样的方法可得到 $V_2' = V_{i_2}$, 对某个异于 i_1 的 i_2. 如此继续下去，最终得到 $m = m'$, 且集合 $\{V_1, \cdots, V_m\}$ 恰为集合 $\{V_1', \cdots, V_m'\}$ 的某一个重新排列. 定理证毕. □

定义 3.2.49 出现在 V 的不可缩不可约分解 (3.2.15) 中的子簇 V_i 称作簇 V 的 *不可约分支*.

定义 3.2.50 簇 V 在 $\mathbf{K}$ 上的 *维数* 定义为 V 的不可约分支在 $\mathbf{K}$ 上维数的最大值.

记号 3.2.51 簇 V 在 $\mathbf{K}$ 上的 *维数* 记作 $\mathrm{Dim}_{\mathbf{K}}\, V$.

问题

注释 3.2.52 本节中的所有定理及其证明都是只具有存在性特点的. 例如，要由 PS 来判断一个簇 $\mathrm{Zero}(PS)$ 是否可约或是否存在母点都不是显而易见的. 因此我们提出下面一些问题，并将在后面几节中研究和解决这些问题.

设 $PS, PS' \subset \mathbf{K}[X]$.

问题 V1 判断一个代数簇 $\mathrm{Zero}(PS)$ 在 $\mathbf{K}$ 上是否不可约.

问题 V2 如果 $\mathrm{Zero}(PS)$ 在 $\mathbf{K}$ 上不可约，找该簇的一个母点.

问题 V3 如果 $\mathrm{Zero}(PS)$ 不是不可约的，确定 $\mathrm{Zero}(PS)$ 的一个不可缩不可约分解.

问题 V4 判断是否有 $\mathrm{Zero}(PS) \subset \mathrm{Zero}(PS')$.

问题 V5 对于 $\mathbf{K}^n$ 中给定的一个扩张点 Ξ, 确定一个多项式集 $PS \subset \mathbf{K}[X]$, 使得 $\mathbf{K}^n$ 中的代数簇 $\mathrm{Zero}(PS)$ 以 Ξ 为母点.

问题 V6 通过多项式集 PS 来研究簇 $\mathrm{Zero}(PS)$ 的结构.

问题 V7 通过多项式集 PS 来研究与簇 $\mathrm{Zero}(PS)$ 相关的计算问题.

射影空间中的射影簇

设射影空间和齐次化多项式等概念与 3.1 节的最后一部分相同.

定义 3.2.53 齐次多项式 ${}^hP \subset \mathbf{K}[{}^hX]$ 的一个齐次零点是指使得 ${}^hP({}^hX') = 0$ 的任一扩张点 ${}^hX'$, 其中 $X' \in P^n_{\mathbf{K}^*}({}^hX)$, $\mathbf{K}^*$ 为 $\mathbf{K}$ 的某一扩域. 一个 *齐次多项式集* 是指一个只含齐次多项式的多项式集. 齐次多项式集的一个 *齐次零点* 是指在该多项式集中的所有齐次多项式的一个公共的齐次零点.

记号 3.2.54 对于齐次多项式集 ${}^hPS \subset \mathbf{K}[{}^hX]$, ${}^hPS$ 的所有齐次零点组

成的集合记作 $\mathrm{Zero}^h({}^hPS)$.

定义 3.2.55 $P^n_{\mathbf{K}}({}^hX)$ 中的以 ${}^hPS \subset \mathbf{K}[{}^hX]$ 为基的一个 *射影簇* 是指集合 $\mathrm{Zero}^h({}^hPS)$, 其中 ${}^hPS$ 为某个齐次多项式集.

例 3.2.56 仍考虑例 3.2.23 中的多项式 $P_1, P_2 \in \mathbf{K}[x_1]$. 设齐次化多项式 ${}^hP_1, {}^hP_2$ 关于 x_1 的结式是 R. 事实上, 这个 R 与例 3.2.23 中的 R 是一样的. 于是有

$$\mathrm{Zero}^h({}^hP_1, {}^hP_2) \neq \emptyset \iff R = 0.$$

注释 3.2.57 将上述结论和 (3.2.12) 相比较, 可以看出, 如果考虑齐次化多项式而不是原来多项式的齐次零点, 零点集可以在结构上变得更简单. 注意到, 这也是为什么特定化 - 扩张定理 (命题 3.1.46) 在射影空间成立而在仿射空间不成立的根本原因.

注释 3.2.58 在射影空间中, 我们可以以通常的方式定义直线, 线性子空间, Pluecker 坐标等概念. 我们也可以在射影空间中定义母线, 母线性子空间等概念. 关于这些概念可参见一些代数几何方面的经典教材, 如 [VdW2] 和 [H-P1,2]. 显然, 对仿射空间也可以自然地定义这些概念.

§3.3 多项式集、升列和偏序

<u>*变量的自然序*</u>

记号 3.3.1 $\mathbf{K}$, $X = (x_1, x_2, \cdots, x_n)$ 和 $X_k = (x_1, \cdots, x_k)$ 的定义如前.

对于变量 $x_1, \cdots, x_n$, 全书将采用如下自然的序, 除非另作说明:

$$x_1 \prec x_2 \cdots \prec x_n.$$

除非另作说明, 下文中的多项式和多项式集都是指在 $\mathbf{K}[X]$ 中.

<u>*多项式的一些指标*</u>

记号 3.3.2 对一个非零多项式 $P \in \mathbf{K}[X]$, 记 $deg_{x_i}(P)$ 为 P 关于 x_i 的次数.

定义 3.3.3 对一个非零多项式 $P \in \mathbf{K}[X]$, P 的 *类* 定义为 P 中出现的 x_c 的最大下标 c; 或 0, 如果 P 是 $\mathbf{K}$ 中一个非零常量. 记作 $cls(P)$.

P 的 *主变元* 定义为 x_c, 如果 P 的类 $c > 0$; 否则不定义. 记作 $lvar(P)$.

P 的 *次数* 定义为 P 关于 x_c 的次数, 如果 P 的类 $c > 0$; 否则定义为 0. 记作 $deg(P)$.

P 的 *长度* 定义为 P 的项数, 并记为 $t(P)$.

P 的 *指标集* 是指 $[t\ c\ d]$, 其中 $t=t(P), c=cls(P), d=deg(P)$, 有时也指 $[t\ u\ d]$, 其中 u 代表变元 x_c.

<u>非常量多项式的正则形式</u>

定义 3.3.4 对一个类为 $c>0$ 的非常量多项式 P, P 称作具有 *正则形式*, 如果

$$P\ =\ I*x_c^d+x_c\text{的低次项}, \tag{3.3.17}$$

其中

$$c=cls(P)>0,\quad d=deg(P)>0,$$

且 x_c 次幂之前的系数都属于 $\mathbf{K}[X_{c-1}]$.

定义 3.3.5 对于正则形式为 (3.3.17) 的非零多项式 P, I 称作 P 的 *初式*, 记作 $init(P)$.

定义 3.3.6 对于类为 $c>0$ 的非零多项式 P, 其形式导数 $\frac{\partial P}{\partial x_c}$ 称作 P 的 *隔离子*, 并记作 $sep(P)$.

约定 对 $\mathbf{K}$ 中的一个非零常量 P, 定义 $init(P)=1$, 但不定义 $sep(P)$.

<u>多项式的偏序关系</u>

设 P,Q 为非零多项式.

定义 3.3.7 称 P 的序 *低于* Q 的序, 或 Q 的序 *高于* P 的序, 如果 $cls(P)<cls(Q)$, 或 $cls(P)=cls(Q)$ 但 $deg(P)<deg(Q)$. 记作: $P\prec Q$ 或 $Q\succ P$.

定义 3.3.8 称 P 和 Q 有 *相同的序*, 如果 $P\prec Q$ 和 $P\succ Q$ 都不成立. 记作 $P\sim Q$.

记号 3.3.9 $P\preceq Q$ 是指 $P\sim Q$ 或 $P\prec Q$.

命题 3.3.10 二元关系 $\prec$ 在 $\mathbf{K}[X]$ 中的所有非零多项式之间引入了一个偏序关系.

证明 只需证明传递性, 即对于任意非零多项式 P_1,P_2,P_3, 有

$$\begin{aligned}
&P_1\prec P_2,\ P_2\prec P_3\Longrightarrow P_1\prec P_3,\\
&P_1\sim P_2,\ P_2\prec P_3\Longrightarrow P_1\prec P_3,\\
&P_1\prec P_2,\ P_2\sim P_3\Longrightarrow P_1\prec P_3,\\
&P_1\sim P_2,\ P_2\sim P_3\Longrightarrow P_1\sim P_3.
\end{aligned}$$

显然, 这些关系可直接由定义得到. □

定义 3.3.11 称 Q 关于 P 是 *约化的*, 如果 $cls(P)=c>0$ 且 $deg_{x_c}(Q)<deg(P)$.

约定 对于 $\mathbf{K}$ 上的非零常量 P, 每一非零多项式关于 P 都不是约化的. 常量 0, 作为一个多项式, 对于任一非零多项式 P, 不管 P 是常量与否, 都是约化的.

升列和三角列

定义 3.3.12 一个多项式集 AS 称作是一个 *升列*, 如果其中的多项式均非零, 且能够排成序列

$$AS: \quad A_1, A_2, \cdots, A_r, \tag{3.3.18}$$

使得下面的 (a_1) 和 (a_2) 成立:

(a_1) $cls(A_1) < cls(A_2) < \cdots < cls(A_r)$,

(a_2) $init(A_j)$ 关于 A_i 是约化的, 对任意的 $i < j$.

因此, 序列 (3.3.18) 称作是 *按升序* 排列的.

定义 3.3.13 一个多项式集 AS 称作一个 *三角列* 或一个 *弱升列*, 如果其中的多项式都非零, 且能够排成序列 (3.3.18), 使得对于按升列排列的序列 (3.3.18), 仅有 (a_1) 成立.

定义 3.3.14 *平凡* 升列或 *平凡* 三角列是指仅由一个非零常量组成的多项式集.

注释 3.3.15 在 (3.3.18) 中, 若 A_1 是 $\mathbf{K}$ 中的非零常量, 则不再出现 $A_2, \cdots, A_r$, 从而升列 AS 必是平凡的. 对一个非平凡的升列, 条件 (a_1) 可以由

$$(a_1)' \qquad 0 < cls(A_1) < cls(A_2) < \cdots < cls(A_r)$$

代替.

定义 3.3.16 一个非平凡升列或三角列 AS 的 *初式积* 是指 AS 中所有多项式的初式的乘积. 记作 $IP(AS)$.

定义 3.3.17 一个非平凡升列或三角列 AS 的 *初式隔离子积* 是指 AS 中所有多项式的初式和隔离子的乘积. 记作 $ISP(AS)$.

升列的偏序关系

设

$$AS': \quad A'_1, A'_2, \cdots, A'_{r'},$$
$$AS'': \quad A''_1, A''_2, \cdots, A''_{r''}$$

是两个按升序排列的升列.

定义 3.3.18 称 AS' 的序 *低于* AS'' 的序或 AS'' 的序 *高于* AS' 的序, 如果以下的 (o_1) 或 (o_2) 之一成立:

(o_1) 存在一个 k, 使得

$$A_1' \sim A_1'', \cdots, A_{k-1}' \sim A_{k-1}'', \text{但 } A_k' \prec A_k''.$$

(o_2) $r' > r''$, 且

$$A_1' \sim A_1'', \cdots, A_{r''}' \sim A_{r''}'',$$

记作 $AS' \prec AS''$ 或 $AS'' \succ AS'$.

定义 3.3.19 称升列 AS', AS'' 有 相等的序, 如果 $AS' \prec AS''$ 和 $AS'' \prec AS'$ 都不成立. 记作 $AS' \sim AS''$.

记号 3.3.20 $AS' \preceq AS''$ 是指 $AS' \prec AS''$ 或者 $AS' \sim AS''$.

定理 3.3.21 二元关系 $\preceq$ 在所有升列之间引入了一个偏序关系.

证明 只需证明序关系的传递性成立, 进一步只需考虑对应于 (o_1) 或 (o_2) 的各种可能情形. □

注释 3.3.22 除了三角列的概念之外，对升列的概念还可作其他不同的改编：用比条件 (a_2) 更强或更弱的条件来代替条件 (a_2). 但在本书中，我们采用现在这个定义.

定义 3.3.23 一个多项式 Q 称作是关于升列 AS约化的, 如果 Q 关于 AS 中的所有多项式都是约化的.

定理 3.3.24 若在一个升列中加入一个关于该升列约化的多项式，则升列的序降低. 确切地说，若在一个升列中加入一个关于该升列约化的多项式，则可从中选取一个升列，其序低于原来的升列.

证明 对于任一个平凡升列，所有的非零多项式关于它都不是约化的. 因此，只须考虑形如 (3.3.18) 的非平凡升列和一个关于该升列约化的非零多项式 R. 先设 $cls(R) < cls(A_1)$. 此时， R 本身就构成一个升列，且其序低于 AS. 再设 $cls(R) = cls(A_k) = c_k$, 对于某个 $0 < k \le r$. 由于 R 关于 AS 是约化的，从而必有 $deg_{c_k}(R) = deg(R) < deg(A_k)$, 故 $R \prec A_k$. 这样，升列

$$AS': \quad A_1, \cdots, A_{k-1}, R$$

的序低于给定升列 AS 的序. 最后设 $cls(R) > cls(A_k), k \le r$ 但 $\le cls(A_{k+1})$. 对 $k < r$, 升列

$$AS': \quad A_1, \cdots, A_k, R$$

的序低于 AS 的序. 定理证毕. □

注释 3.3.25 这一定理给出了一种可获得比给定升列的序更低的一个升列的方法，即向其中添加关于该升列约化的多项式. 它也显示了条件 (o_2) 在

升列的偏序中所起的作用. 由于升列 AS 中任意一个多项式的初式关于 AS 都是约化的, 从而可选取 R 为任一个这样的初式来得到一个序更低的升列. 这也显示了条件 (a_2) 在升列的定义中所起的作用.

定理 3.3.26 序不断降低的升列序列是有限的.

证明 考虑一个升列序列

$$AS_1 \succeq AS_2 \succeq \cdots \succeq AS_q \succeq \cdots , \tag{3.3.19}$$

则只需证明, 对这样的一个序列存在指标 q, 使得 q 之后的所有升列都有相同的序. 为此设每一 AS_q 按升序有如下排列:

$$AS_q: \ A_{q1}, \cdots, A_{qr_q}, \tag{3.3.20}$$

其中所有的 $r_q \leq n$ 且 ≥ 1. 令 $\max(r_q) = r$, 对 r 作归纳. 考虑由这些升列的第一个多项式组成的序列

$$A_{11}, A_{21}, \cdots, A_{q1}, \cdots . \tag{3.3.21}$$

于是, 这一序列的每一个多项式的序都高于或者等于其后的多项式的序. 因此, 这些多项式的类不会无限增加, 从而在某一步之后多项式都有相同的类. 记这个相同的类为 c_1. 在这一步之后, 这些多项式关于 x_{c_1} 的次数不会无限增加, 于是在这一步后面的另一步之后, 所有多项式关于 x_{c_1} 的次数相同, 因此有相同的序. 设这一步为 q_1. 若 $r = 1$, (3.3.20) 中的所有升列在第 q_1 步之后都有相同的序, 故定理在 $r = 1$ 时成立. 现设定理在 $r = k \geq 1$ 时成立, 我们考虑 $r = k + 1$ 的序列 (3.3.20). 令 AS'_q 为 AS_q 中去掉第一个多项式 A_{q1} 后得到的升列. 设 q_1 是通过上面的 (3.3.21) 得到的, 于是有

$$AS'_{q_1} \succeq AS'_{q_1+1} \succeq \cdots \succeq AS'_{q'} \succeq \cdots , \tag{3.3.22}$$

其中相应的 r_q 和 r 分别为 $r'_q = r_q - 1$ 和 $r' = \max(r'_q) \leq k$. 若在某一步之后所有的 $r'_{q'}$ 都为零, 那么给定序列 (3.3.19) 中的升列在这一步之后都将有相同的序, 从而定理得证. 假设不是这种情形, 去掉 (3.3.22) 中所有这样的 AS'_q, 其中 $r'_q = 0$, 仍得到一个升列的无限序列. 由归纳假设, 所有升列在某一步之后有相同的序. 这一结论对原来的序列也是正确的, 因此定理得证. □

<u>*多项式集的偏序*</u>

定义 3.3.27 包含在多项式集 PS 中的序最低的任一升列称作 PS 的一个*基列*.

定理 3.3.28 一个多项式集的任意两个基列有相同的序.

证明 直接由定义可得. □

从定理 3.3.28, 可以看出如下定义是合理的.

定义 3.3.29 对于任意两个多项式集 PS', PS'', BS', BS'' 分别是 PS', PS'' 的任一基列. 称 PS' 的序低于, 高于, 不高于或等于PS'' 的序, 如果 BS' 的序低于, 高于, 不高于或等于 BS'' 的序. 记作: $PS' \prec PS'', PS' \succ PS'', PS' \preceq PS''$ 或 $PS' \sim PS''$.

下面的定理 3.3.30~3.3.32 可直接由相应的升列定理得到.

定理 3.3.30 二元关系 $\prec$ 在所有多项式集之间引入了一个偏序关系.

定理 3.3.31 若在一个多项式集中添加一个关于它的一个基列约化的多项式, 则这个多项式集的序会降低.

定理 3.3.32 序不断下降的多项式集序列是有限的.

余式和余式公式

设 F, G 为非零多项式, $c = cls(F), I = init(F)$. 通过作简单的除法, 我们得到某一非负整数 s 和多项式 Q, R, 使得

$$I^s * G = Q * F + R, \tag{3.3.23}$$

其中 R 关于 F 是约化的. 我们可选取尽可能小的指数 s 使得上述公式成立, 于是多项式 R 是唯一的.

定义 3.3.33 当 s 的选取尽可能小时, (3.3.23) 中的 R 称作 G 关于 F 的余式. 记作: $R = \mathrm{Remdr}(G/F)$.

注释 3.3.34 设 $R \neq 0$, 且 x_e 在 R 中出现, 其中 $e > c$, 则 $deg_{x_e}(R) = deg_{x_e}(G)$.

注释 3.3.35 在 (3.3.23) 中, 若 $c = 0$ 或 F 是 $\mathbf{K}$ 中的一个非零常量, 则 $R = 0$, $s = 0, Q = \frac{G}{F}$. 因此, $\mathrm{Remdr}(G/F) = G$. 若 $c > 0$ 且 $deg_{x_c}(G) < deg(F)$, 那么 $s = 0, Q = 0$ 且 $R = G$, 从而 $\mathrm{Remdr}(G/F) = G$, 且 G 关于 F 约化.

注释 3.3.36 此处的余式概念来源于 J. F. Ritt 的著作, 它不同于通常一些文献中 伪余式 的概念, 在伪余式中取 s 为 $\max(deg_{x_c}(G) - deg(F) + 1, 0)$, 其中 $cls(F) = c > 0$. 本书中将采用 Ritt 的概念, 除非另外说明.

定理 3.3.37 对一个按照升序排列的升列 (或三角列) AS 以及任一非零多项式 G, 存在唯一确定的关于 AS 约化的多项式 R, 使得

$$I_G * G \equiv R \ \mathrm{mod}_{\mathbf{K}}\ AS,$$

或 (3.3.24)

$$I_G * G = \sum_i Q_i * A_i + R,$$

其中 Q_i 是一些多项式, I_G 是 AS 中多项式 A_i 的初式的幂积.

证明 设 I_i 是 (3.3.18) 中多项式 A_i 的初式. 令 $R_r = G$. 运用 (3.3.23), 以相反的次序连续地作 G 关于 (3.3.18) 中的多项式 A_i 的余式, 我们依次得到一组惟一的非负整数 s_i, 多项式 Q'_i, R_i, $i = r, r-1, \cdots, 2, 1$, 其中 R_i 是满足如下方程的相应的余式:

$$\begin{aligned} I_r^{s_r} * R_r &= Q'_r * A_r + R_{r-1}, \\ I_{r-1}^{s_{r-1}} * R_{r-1} &= Q'_{r-1} * A_{r-1} + R_{r-2}, \\ &\cdots, \\ I_1^{s_1} * R_1 &= Q'_1 * A_1 + R_0. \end{aligned} \tag{3.3.25}$$

令 $R_0 = R$, 则得到如下形式的表达式:

$$I_1^{s_1} * \cdots * I_r^{s_r} * G = \sum_i Q_i * A_i + R,$$

其中每个 Q_i 是 Q'_j 与一些初式 I_k 的幂积的和. 这即为公式 (3.3.24). 由于每个 R_i 是唯一确定的, 从而 R 也是唯一确定的. 由注释 3.3.34 知, R 关于 AS 是约化的. □

定义 3.3.38 (3.3.24) 中唯一确定的多项式 R 称作 G 关于 AS 的 *余式*. 记作: $\mathrm{Remdr}(G/AS)$. 公式 (3.3.24) 称作 G 关于 AS 的 *余式公式*.

定义 3.3.39 对于一个多项式集 PS, PS 中的多项式关于升列 AS 的余式组成的集合称作 PS 关于 AS 的 *余式集*. 记作: $\mathrm{Remdr}(PS/AS)$.

注释 3.3.40 对于一个升列 AS, (3.3.24) 中的余式 R 关于 AS 是约化的. 由定理 3.3.31 知, 如果向一个多项式集加进一个多项式, 该多项式是某一多项式关于该多项式集的任一基列的非零余式, 则原多项式集的序将降低. 这一结论构成了下一节所描述的方法的基本原理, 这一方法是我们整个理论的基石.

平方余式和平方余式公式

考虑到在最优化问题和后面几章中其他问题上的应用, 其中 $\mathbf{K} = \mathbf{R}$, 我们对余式和余式公式的概念作如下改动.

在 (3.3.23) 中, 限制 s 为非负偶整数 $2 * s'$. 选取 s 尽可能小, 使得 (3.3.23) 变为

$$I^{2*s'} * G = Q' * F + R'. \tag{3.3.26}$$

我们也可将 (3.3.24) 用下面的方程代替:

$$I'_G * G \equiv R' \ \mathrm{mod}_{\mathbf{K}}\ AS,$$

或

$$I'_G * G = \sum_i Q'_i * A_i + R'. \tag{3.3.27}$$

在 (3.3.27) 中， I'_G 是 AS 中 A_i 的初式的偶次幂的乘积. 于是，对应于定义 3.3.39, 我们有如下定义：

定义 3.3.41 (3.3.26) 中唯一确定的多项式 R' 称作 G 关于 AS 的 *平方余式*.记作：$Sq\text{-Remdr}(G/AS)$. 公式 (3.3.27) 称作 G 关于 AS 的 *平方余式公式*.

一些例子

例 3.3.42 考虑 §1.2 中朱世杰的例子. 我们有多项式集 $PS = \{P_1, P_2, P_3\}$, 其中 P_i 如下给出：

$$\begin{aligned} P_1 &= x * y * z - x * y^2 - z - x - y, \\ P_2 &= x * z - x^2 - z - y + x, \\ P_3 &= z^2 - x^2 - y^2. \end{aligned}$$

按照朱世杰解相应方程的方法，变元的序为

$$z \prec x \prec y.$$

这相当于

$$z = x_1, \quad x = x_2, \quad y = x_3.$$

于是有

$$\begin{aligned} cls(P_1) = 3,\ deg(P_1) = 2, \\ cls(P_2) = 3,\ deg(P_2) = 1, \\ cls(P_3) = 3,\ deg(P_3) = 2. \end{aligned}$$

包含在 PS 中的升列仅有 3 个，即

$$AS_1 = \{P_1\},\ AS_2 = \{P_2\},\ AS_3 = \{P_3\}.$$

显然，唯一的基列为升列 AS_2.

例 3.3.43 考虑多项式集 $PS = \{P_1, P_2, P_3\}$, 其中 P_i 如下给出：

$$P_i = a_i * x + b_i * y + c_i * z - d_i, \quad i = 1, 2, 3,$$

这里 a_i, b_i, c_i 是 $\mathbf{K}$ 中的非零常量. 无论变量 x, y, z 的序如何，都有 3 个升列 $AS_i, i = 1, 2, 3$, 其中

$$AS_i = \{P_i\}, \quad i = 1, 2, 3.$$

显然，其中的任何一个都是 PS 的一个基列. 由此可知，一个多项式集的基列通常不唯一.

胡森和王东明的一些定理

设 U 为参数集 $(u_1, \cdots, u_d)$, 它可以为空. 现考虑域 $\mathbf{K} = \mathbf{Q}$ 上的由 (3.3.18) 给出的升列 AS, 且 $cls(A_i) = c_i$, U 看作参数.

记号 3.3.44 在 (3.3.18) 给出的 AS 中：

$X' :=$ 限制变元 $x_{c_i}, i = 1, \cdots, r$.

$X'' :=$ 自由变元集 $X \setminus X'$.

定义 3.3.45 $\mathbf{K}$ 上的升列 (3.3.18) 称作是 *完全的*(或关于 X *不完全*), 如果 $X'' = \emptyset$(或 $\neq \emptyset$).

下面的定理是胡森和王东明得到的有关多变元多项式在任意扩域上的分解定理. 我们将在后面的 4.5 节中讨论这一定理. 参见 [H-W] 和 [WDM1].

定理 3.3.46 设 $AS = \{A_1, \cdots, A_r\}$ 为 $\mathbf{Q}[X, U]$ 中的一个升列，IP 是其初式积. 若 AS 关于 X 不是完全的，则或是 $\mathrm{Zero}_{\mathbf{C}}(AS/IP)$ 为空，或 $\mathbf{C}$ 中有值 $U = U^0$, 使得对于 $U = U^0$, $\mathrm{Zero}_{\mathbf{C}}(AS/IP)$ 是无限的.

证明 设 $\mathrm{Zero}_{\mathbf{C}}(AS/IP) \neq \emptyset$, 则有零点 $U = U^0, X'' = X''^0$. 于是由代数方程的根对其系数的连续性，当 X'' 任意接近于 X''^0 时，$\mathrm{Zero}_{\mathbf{C}}(AS/IP)$ 都有零点 $U = U^0$. 由于 X'' 非空，集合 $\mathrm{Zero}_{\mathbf{C}}(AS/IP)$ 对于 $U = U^0$ 是个无限集. □

定理 3.3.47 设 AS, IP 如定理 3.3.46 所述. 若 AS 是完全的，则 $\mathrm{Zero}_{\mathbf{Q(U)}}(AS/IP)$ 或等于 $\emptyset$ 或是有限的，并且可由 Gauss 引理确定.

证明 直接由定义和 Gauss 引理可得. □

§3.4 多项式集的特征列和整序原理

问题，原理和方法

下文中的 $\mathbf{K}, X = (x_1, \cdots, x_n), X_k = (x_1, \cdots, x_k)$ 等如前所述. 多项式和多项式集都看作在 $\mathbf{K}[X]$ 中. 一个多项式集 PS 的 *零点结构* 是指 PS 的零点集的结构，即簇 $\mathrm{Zero}(PS)$ 的结构.

问题 Z 通过 $\mathrm{Zero}(PS)$ 的基 PS 来研究簇 $\mathrm{Zero}(PS)$ 的结构.

原理和方法 我们认为一个升列的零点结构已经确定. 于是，我们通过研究多项式集 PS 中序最低的升列，即基列，来研究 PS 的零点结构. 根据定理 3.3.24 和定理 3.3.31, 多项式集的基列可以通过加进某些多项式关于该基列的非零余式来降序. 这就给出了一种构造序尽可能低的基列的方法：通过尽可能

地往多项式集中添加非零余式，直到得到某一特殊类型的升列 (在下文中称作特征列) 为止.

特征列和它的构造图表

给定一个多项式集 PS, 我们来研究它的零点结构. 根据上面所述的原理和方法，先设 $PS_0 = PS$, 任取 PS 的一个基列 BS_0. 若仍然存在多项式属于 PS_0 但不属于 BS_0, 求出这些多项式关于 BS_0 的余式. 假设有非零余式且它们组成一个非空集合 RS_0, 则得到一个新的多项式集 $PS_1 = PS_0 + BS_0 + RS_0$. 再任取 PS_1 的一个基列 BS_1. 根据定理 3.3.24 和 3.3.31, $BS_0 + RS_0$ 的序比 BS_0 的序低，因而 PS_1 或 BS_1 的序比 BS_0 的序低. 若 PS_1 关于 BS_1 的余式中存在非零余式，记 RS_1 为所有这些非零余式组成的集合. 假设 RS_1 非空，同理可构造多项式集 $PS_2 = PS_0 + BS_1 + RS_1$, 基列 BS_2 和余式集 RS_2. 只要余式集非空，就可以继续做下去. 于是有

$$BS_0 \succ BS_1 \succ BS_2 \succ \cdots .$$

根据定理 3.3.26, 这一序列只能是有限的. 因而, 在某一步 m 时将得到 $RS_m = \emptyset$. 因此, 最后得到的基列 BS_m 是一个与给定多项式集 PS 有关的升列, 记作 CS.

以上的过程可以用下面的图表 (S) 来表示:

$$\left.\begin{array}{llllll} PS = & PS_0 & PS_1 & \cdots & PS_i & \cdots \quad PS_m \\ & BS_0 & BS_1 & \cdots & BS_i & \cdots \quad BS_m = CS \\ & RS_0 & RS_1 & \cdots & RS_i & \cdots \quad RS_m = \emptyset. \end{array}\right\} \tag{S}$$

在图表 (S) 中，所有的余式集 RS_k 非空，这里 $k < m$. 我们记

$$\left.\begin{array}{l} BS_i \ = PS_i \text{ 的一个基列}, \\ RS_i = \mathrm{Remdr}(PS_i \setminus BS_i \ / \ BS_i) \setminus \{0\}, \\ PS_i = PS_0 + BS_{i-1} + RS_{i-1}. \end{array}\right\} \tag{3.4.28}$$

定理 3.4.1 图表 (S) 中的步骤将在有限的 m 步之后终止, 此时相应的余式集 $RS_m = \emptyset$. 于是相应的基列 $BS_m = CS$ 满足下列性质 (c_1) 和 (c_2):

(c_1) $\mathrm{Remdr}(PS/CS) = \{0\}$,

(c_2) $\mathrm{Zero}(PS) \subset \mathrm{Zero}(CS)$.

证明 我们已经证明了以上步骤将在有限步之后终止. 于是在某一步 m 时，图表中的 $RS_m = \emptyset$. 为证 $CS = BS_m$ 满足 (c_1) 和 (c_2), 首先注意到 $CS \subset PS_m$, 于是

$$\mathrm{Zero}(PS_m) \subset \mathrm{Zero}(CS). \tag{3.4.29}$$

由构造过程知

$$\text{Remdr}(PS_m/CS) = \{0\}. \tag{3.4.30}$$

特别地，(c_1) 成立，因为 $PS = PS_0 \subset PS_m$. 为证 (c_2), 首先对 k 施用归纳法，证明

$$\text{Zero}(PS) = \text{Zero}(PS_0) = \text{Zero}(PS_k), \quad k = 1, \cdots, m. \tag{3.4.31}$$

注意到，$PS_1 = PS_0 + BS_0 + RS_0$. 考虑 RS_0 中的任一个多项式 R_0, 则 R_0 是 $PS_0 \setminus BS_0$ 中的某一多项式关于 BS_0 的非零余式. 根据余式公式 (3.3.24), 我们有如下形式的等式:

$$I_{P_0} * P_0 = \sum_i Q_i * B_i + R_0,$$

其中 B_i 为 BS_0 中的多项式，I_{P_0} 是多项式 B_i 的初式的方幂的乘积. 由这一公式知，PS_0 和 BS_0 的任一零点都是 RS_0 的一个零点，因此

$$\text{Zero}(PS_1) = \text{Zero}(PS_0 + BS_0 + RS_0) = \text{Zero}(PS_0 + BS_0) = \text{Zero}(PS_0).$$

这样就对 $k = 1$ 的情形证明了 (3.4.31). 假设对 k 的情形我们已经证明了 (3.4.31). 考虑多项式集 $PS_{k+1} = PS_0 + BS_k + RS_k$. 同前，由 $PS_k \setminus BS_k$ 中多项式关于 BS_k 的余式公式知，$\text{Zero}(PS_k + BS_k + RS_k) = \text{Zero}(PS_k + BS_k) = \text{Zero}(PS_k)$. 由于 $\text{Zero}(PS_0) = \text{Zero}(PS_k)$, 于是有

$$\begin{aligned}\text{Zero}(PS_{k+1}) &= \text{Zero}(PS_0 + BS_k + RS_k) = \text{Zero}(PS_k + BS_k + RS_k) \\ &= \text{Zero}(PS_k) = \text{Zero}(PS_0).\end{aligned}$$

因此，(3.4.31) 对 $k+1$ 的情形也成立. 又由 (3.4.29), (c_2) 成立. □

<u>特征列</u>

定义 3.4.2　多项式集 PS 的一个 *特征列* 是指按照某一图表 (S) 中的步骤，由 PS 得到的任一升列 CS. 更一般地说，多项式集的 *特征列* 是指满足定理 3.4.1 中性质 (c_1) 和 (c_2) 的任一升列 CS. CS 中的多项式称为 CS 的 *特征多项式*.

注释 3.4.3　若特征列 CS 是平凡的, 即只含有一个非零常量, 则 $\text{Zero}(PS) = \emptyset$.

注释 3.4.4　对于多项式集 PS 的一个特征列 CS, 并不要求 CS 中的多项式在 PS 中. 然而，从过程中可以看出 CS 中的多项式都在以 PS 的多项式为基的生成理想中.

注释 3.4.5 这里确定的多项式集 PS 的特征列 CS 不是唯一的，因为在图表 (S) 的每一步中，基列的选取都不唯一. 参见例 3.3.43.

注释 3.4.6 特征列的概念和术语出自 J. F. Ritt 的著作，参见 [Ritt1, 2]. 然而，正如 D. Kapur 向本书作者指出的那样，Ritt 定义的特征列只是对理想而言，而这里的特征列是对多项式集或理想的基定义的.

注释 3.4.7 在原来的图表 (S) 中，我们用的是关系式 $PS_i = PS_{i-1} + BS_{i-1} + RS_{i-1}$, 而不是 $(3.4.28)_3$. 在吴文达和支丽红的建议下，我们作了上述改变，从而大大地简化了计算.

<u>*特征列算法*</u>

从图表 (S) 可以看出，多项式集 PS 的一个特征列 CS 可以由下面的算法确定.

特征列算法:

输入：一个多项式集 PS.

输出：PS 的一个特征列 CS.

第 1 步：令 $PS_0 \longleftarrow PS$.

第 2 步：取 PS_0 的一个基列 BS.

第 3 步：构造 $RS = \mathrm{Remdr}(PS_0 \setminus BS/BS) \setminus \{0\}$.

第 4 步：若 $RS = \emptyset$, 则 $CS \longleftarrow BS$, 返回. 否则，$PS_0 \longleftarrow PS + BS + RS$. 转到第 2 步.

第 2 步可以通过如下算法得到:

基列算法:

输入：一个多项式集 PS.

输出：PS 的一个基列 BS.

第 1 步：设 $PS' = PS$ 且 $BS = \emptyset$.

第 2 步：若 $PS' = \emptyset$, 返回 BS. 否则，从 PS' 中取出类和次数都最小的多项式 B, 令 $BS \longleftarrow BS + \{B\}$.

第 3 步：令 $PS' \longleftarrow PS'$ 中关于 B 约化的所有多项式组成的集合.

第 4 步：转到第 2 步.

<u>*整序原理*</u>

由定理 3.4.1 可推导出如下定理 3.4.8. 该定理指出了一个给定多项式集的零点结构和它的特征列之间的密切关系. 它在我们的整个理论中占有重要的地位. 因此，我们把这个定理命名为整序原理. 后面将会看到，它在各种应用

中将发挥重要的作用.

定理 3.4.8 (整序原理) 设 CS 为多项式集 PS 的一个特征列, 则

$$\left.\begin{aligned}&\mathrm{Zero}(CS/IP) \subset \mathrm{Zero}(PS) \subset \mathrm{Zero}(CS),\\&\mathrm{Zero}(PS/IP) = \mathrm{Zero}(CS/IP),\\&\mathrm{Zero}(PS) = \mathrm{Zero}(CS/IP) + \textstyle\bigcup_i \ \mathrm{Zero}(PS + \{I_i\}).\end{aligned}\right\} \tag{3.4.32}$$

在 (3.4.32) 中, I_i 为 CS 中多项式 C_i 的初式, IP 是 CS 的初式积. 此外, CS 的序不会高于 PS 的序.

证明 对任一 $P \in PS$, 由性质 (c_1) 有 $\mathrm{Remdr}(P/CS) = 0$. 因此由对 P 的余式公式 (3.3.24), 我们有

$$I_P * P = \sum_i Q_{iP} * C_i, \tag{3.4.33}$$

其中 Q_{iP} 是多项式, I_P 是 I_i 的某一幂积. 由此有

$$\mathrm{Zero}(CS/IP) \subset \mathrm{Zero}(CS/I_P) \subset \mathrm{Zero}(P).$$

因为上式对 PS 中的所有多项式 P 都成立, 我们有

$$\mathrm{Zero}(CS/IP) \subset \mathrm{Zero}(PS).$$

由性质 (c_2), 我们得到 $(3.4.32)_1$ 和 $(3.4.32)_2$. 由于

$$\mathrm{Zero}(PS) = \mathrm{Zero}(PS/IP) + \mathrm{Zero}(PS + \{IP\}),$$

容易由 $(3.4.32)_2$ 得到 $(3.4.32)_3$. 由 CS 的构造, 最后的结论是显然的. 定理证毕. □

<u>特征列算法的变形</u>

另一种按照图表 (S) 确定特征列的步骤是用下面的 (3.4.34) 来代替 $(3.4.28)_3$:

$$PS_i = BS_{i-1} + RS_{i-1}. \tag{3.4.34}$$

改用 (3.4.34) 后, 整个过程仍然会在有限步, 比如说第 m 步之后终止, 此时 $RS_m = \emptyset$. 最后的基列 $BS_m = CS$ 一般不满足性质 $(c_1), (c_2)$, 从而也不满足性质 (3.4.32). 只有在下面定理中的条件 (3.4.35) 成立时, 基列才会仍满足这些性质.

定理 3.4.9 在图表 (S) 中采用 (3.4.34) 来代替 $(3.4.28)_3$ 后, 最后得到的基列 $BS_m = CS$ 满足性质 $(c_1), (c_2)$, 从而是 PS 的特征列当且仅当下列条件成立:

$$\mathrm{Remdr}(PS/CS) \ = \ \{0\}. \tag{3.4.35}$$

证明 该证明实际上和定理 3.4.1 的证明相同，在此略. □

现在假设 (3.4.35) 不成立. 我们构造一个新的多项式集

$$PS' = CS + RS,$$

其中

$$RS = \text{Remdr}(PS/CS) \setminus \{0\}.$$

再对 PS' 运用特征列的算法，用 (3.4.34) 代替 $(3.4.28)_3$. 整个过程按如下图表一步一步进行下去：

$$\begin{aligned} PS \ &\underset{(S)}{\longrightarrow} CS \longrightarrow PS' \underset{(S)}{\longrightarrow} CS' \longrightarrow \cdots \\ &\underset{(S)}{\longrightarrow} CS^{(i-1)} \longrightarrow PS^{(i-1)} \underset{(S)}{\longrightarrow} CS^{(i)} \longrightarrow \cdots . \end{aligned} \tag{S$'$}$$

在图表中，记

$$\begin{aligned} PS^{(i)} &= CS^{(i-1)} + RS^{(i-1)}, \\ RS^{(i)} &= \{\text{Remdr}(PS/CS^{(i)})\} \setminus \{0\}. \end{aligned} \tag{3.4.36}$$

定理 3.4.10 过程 (S)$'$ 必将在有限步之后停止，此时对于某个 k 有 $RS^{(k)} = \emptyset$. 于是 $CS^{(k)}$ 满足性质 $(c_1),(c_2)$, 因而是 PS 的特征列.

证明 由定理 3.3.24 和 3.3.31 可得. 证明与定理 3.4.1 类似. □

定义 3.4.11 用 (3.4.34) 代替 $(3.4.28)_3$ 后，图表 (S)$'$ 中的步骤**验证**是指验证 (3.4.35) 是否正确.

注释 3.4.12 定理 3.4.9 表明，用 (3.4.34) 代替 $(3.4.28)_3$ 后，若验证是正确的，那么最后得到的基列 CS 将是所求的特征列. 只有当验证不正确时，我们才不得不按图表 (S)$'$ 继续做下去.

注释 3.4.13 在实际的计算中，图表 (S)$'$ 比图表 (S) 更常用.

用 (3.4.34) 代替 $(3.4.28)_3$ 后，关于怎样适当地修改特征列算法我们已经很清楚了.

<u>关于 (3.4.34) 的整序原理的扩展形式</u>

在图表 (S) 中用 (3.4.34) 代替 $(3.4.28)_3$ 后，公式 (3.4.32) 不再成立，但是可以用更复杂的形式来代替. 特别地， $(3.4.32)_3$ 可以用下面定理中的公式 (3.4.37) 来代替.

定理 3.4.14 在图表 (S) 中用 (3.4.34) 后，我们有

$$\text{Zero}(PS) = \text{Zero}(CS/K_m) + \bigcup_{k=0}^{m} \text{Zero}(PS_k/K_{k-1}), \tag{3.4.37}$$

且

$$\left.\begin{aligned} J_k &= IP(BS_k), \\ K_k &= J_0 * J_1 * \cdots * J_k, \\ PS_k &= PS + \{J_k\}. \end{aligned}\right\} \tag{3.4.38}$$

证明 对 k 施用归纳法. 证明参见原始文献 [WWT13]. □

朱世杰的一个例子

例 3.4.15 考虑例 3.3.42 中朱世杰给出的例子. 变量序为 $z \prec x \prec y$, 这相当于 $z = x_1, x = x_2, y = x_3$, 我们有 $PS = PS_0 = \{P_1, P_2, P_3\}, BS_0 = \{P_2\}$, 其中多项式 P_i 如下给出:

$$\begin{aligned} P_1 &= x * y * z - x * y^2 - z - x - y, \\ P_2 &= x * z - x^2 - z - y + x, \\ P_3 &= z^2 - x^2 - y^2. \end{aligned}$$

容易得到

$$\begin{aligned} R_{01} &= \text{Remdr}(P_1/BS_0) \\ &= x * (-x^4 + 2 * x^3 * z + 2 * x^3 - x^2 * z^2 \\ &\quad -5 * x^2 * z - x^2 + 3 * x * z^2 + 3 * x * z + x - 2 * z^2 - z - 2), \\ R_{02} &= \text{Remdr}(P_3/BS_0) \\ &= x * (-x^3 + 2 * x^2 * z + 2 * x^2 - x * z^2 - 4 * x * z - 2 * x + 2 * z^2 + 2 * z). \end{aligned}$$

因此, $RS_0 = \{R_{01}, R_{02}\} \neq \emptyset$. 使用 (3.4.34), 按照图表 (S) 做下去, 就可得到

$$PS_1 = BS_0 + RS_0 = \{P_2, R_{01}, R_{02}\}. \tag{3.4.39}$$

这一过程将在第 $m = 5$ 步时停止, 我们最后得到 $RS_5 = \emptyset, PS_5 = BS_5 = CS = \{C_1, C_2\}$, 其中 C_1,C_2 如下给出:

$$\left.\begin{aligned} C_1 &= x * (z-1)^2 * (z+1) * (z-5), \\ C_2 &= -y - x^2 + x * z + x - z. \end{aligned}\right\} \tag{3.4.40}$$

容易验证: P_i 关于 CS 的余式都为 0. 因此由定理 3.4.9 有

$$CS = \{C_1, C_2\} \tag{3.4.41}$$

是 PS 的一个特征列. 又由整序原理 (3.4.32) 知

$$\text{Zero}(PS) = \text{Zero}(CS/I_1) + \text{Zero}(PS + \{I_1\}), \tag{3.4.42}$$

其中

$$I_1 = (z-1)^2 * (z+1) * (z-5) \tag{3.4.43}$$

是 C_1 的初式.

关于多余因子的 Collins- 李现象

给定两个多项式 $F, G \in \mathbf{K}[x]$, 其系数在唯一分解整环 $\mathbf{D}$ 中. 构造如下序列:

$$F_0, F_1, F_2, \cdots, F_r,$$

其中 $F_0 = F, F_1 = G$, 每一个 $F_i (i \geq 3)$ 是 F_{i-1} 关于 F_{i-2} 的伪余式, 最后的 F_r 在 $\mathbf{D}$ 中. Collins 已经发现了一个重要的现象, 即只要 i 充分大, F_i 之前的所有多项式的首项系数是 F_i 的首项系数的因子. 参见 [Coll] 及 [B-T]. 当伪余式用定义 3.3.33 中的余式代替时, 此性质仍然成立.

李子明已经把 Collins 的发现推广到了特征列构造的情形. 他证明了 (参见 [LZM1, 2, 3]), 至少在一般情况下, 图表 (S) 中的余式必将以它之前的基列中的多项式的初式为因子. 关于 Collins 和李子明的定理, 可参见他们的原始论文. 我们仅仅指出, 由于这些因子的出现是不可避免的, 整个过程中的多项式将会变得非常大, 这就使得后面的计算难以进行下去. 此外, 其他意想不到的因子也可能在过程中出现, 就像例 3.4.15 中出现 R_{01}, R_{02} 的因子 x 和其他因子一样. 因此有必要在步骤中去掉所有这样的因子, 不论它是不是基列的初式, 以使多项式的个数变少. 去掉这些因子对特征列的影响可从下文看到.

特征集和整序原理的推广

定义 3.4.16 多项式集 PS 模多项式 F 的 *特征列* 是指一个满足如下性质 (c_1') 和 (c_2') 的升列 CS':

$(c_1)'$ $\mathrm{Remdr}(PS/CS') = \{0\}$,

$(c_2)'$ $\mathrm{Zero}(PS/F) \subset \mathrm{Zero}(CS'/F)$.

定理 3.4.17 设 CS' 是多项式集 PS 模 F 的特征列, 则

$$\left.\begin{array}{l} \mathrm{Zero}(CS'/IP * F) \subset \mathrm{Zero}(PS/F) \subset \mathrm{Zero}(CS'/F), \\ \mathrm{Zero}(PS/IP * F) = \mathrm{Zero}(CS'/IP * F), \\ \mathrm{Zero}(PS/F) = \mathrm{Zero}(CS'/IP * F) + \bigcup_i \mathrm{Zero}(PS + \{I_i'\}/F), \\ \mathrm{Zero}(PS) = \mathrm{Zero}(PS/F) + \mathrm{Zero}(PS + \{F\}). \end{array}\right\} \tag{3.4.44}$$

在 (3.4.44) 中, I_i' 为 CS' 中多项式 C_i' 的初式, IP' 是 CS' 的初式积.

特征列算法如前, 但是在步骤中, 因子 F_j 可以去掉. 最后得到的升列 $BS_m = CS'$ 就是 PS 模 $F = \Pi_j F_j$ 的特征列.

注释 3.4.18 对于这种模一些因式的情形，定理 3.4.9 及其验证可类似地叙述，在此略.

进一步运用 (3.4.44), 其中 F 是所有隔离子的乘积，则由 $(3.4.32)_3$ 容易得到整序原理的另一个有用推广.

定理 3.4.19 (修改后的整序原理) 设 CS 是 PS 的一个特征列，其中 PS 的初式隔离子积为 ISP, 则

$$\text{Zero}(PS) = \text{Zero}(CS/ISP) + \bigcup_i \text{Zero}(PS + \{I_i\}) + \bigcup_i \text{Zero}(PS + \{S_i\}). \tag{3.4.45}$$

在 (3.4.45) 中，I_i, S_i 分别是 CS 中特征多项式的初式和隔离子.

一些例子

例 3.4.20 仍考虑例 3.4.15. 在 (3.4.39) 的 PS_1 中，多项式 R_{01}, R_{02} 显然有因子 x. 如果我们假设 $x \neq 0$, 就可以把因子 x 从 R_{01}, R_{02} 中消去，得到 $R'_{01} = R_{01}/x, R'_{02} = R_{02}/x$. 于是有多项式集 $\{P_2, R'_{01}, R'_{02}\}$, 在图表 (S) 中使用 (3.4.34), 并继续做下去. 算法将在第 $m = 4$ 步之后停止. 最后得到的基列 $BS'_4 = \{B'_1, B'_2, B'_3\}$ 如下给出：

$$\begin{aligned}
B'_1 &:= (z-1)^2 * (z+1) * (z-5), \\
B'_2 &:= x * z^2 - 3 * x * z - 7 * x - z^3 + 3 * z^2 + 7 * z + 6, \\
B'_3 &:= -y - x^2 + x * z + x - z.
\end{aligned}$$

通过验证知，P_1, P_3 关于 BS'_4 的余式均非零. 于是把这些非零余式加到 PS 中，并按图表 (S)$'$ 继续做下去. 我们最终得到，PS 模 x 的特征列为 $CS' = \{C'_1, C'_2, C'_3\}$, 这里

$$\left.\begin{aligned}
C'_1 &= (z+1) * (z-5), \\
C'_2 &= x * (z-2) - 2 * z + 1, \\
C'_3 &= -y - x^2 + x * z + x - z.
\end{aligned}\right\} \tag{3.4.46}$$

由整序原理，模去因子 $(3.4.44)_3$ 后，我们得到

$$\left.\begin{aligned}
\text{Zero}(PS) &= \text{Zero}(PS/x) + \text{Zero}(PS + \{x\}), \\
\text{Zero}(PS/x) &= \text{Zero}(CS'/x * (z-2)) + \text{Zero}(PS + \{z-2\}/x).
\end{aligned}\right\} \tag{3.4.47}$$

例 3.4.21 下面的例子选自 Czapor 和 Geddes 的文章 [C-G]. 考虑一个多项式集 $PS = \{P_1, P_2, P_3\}$, 其中

$$\left.\begin{aligned}P_1 &= x^2 + a*y*z + d*x + g,\\ P_2 &= y^2 + b*z*x + e*y + h,\\ P_3 &= z^2 + c*x*y + f*z + k,\end{aligned}\right\} \tag{3.4.48}$$

这里的 a, b 等被视作独立参数. 变量序 $x \prec y \prec z$ 相当于 $x = x_1, y = x_2, z = x_3$. 设 $PS = PS_0$. 令 $BS_0 = \{B_{01}\}$, 其中 $B_{01} = P_2$. 按照 (3.4.34) 的特征列算法做下去, 在步骤中消去因子

$$F_1 = x,\ F_2 = x*b*f - h, \tag{3.4.49}$$

最后得到一个基列 $BS_5 = CS = \{C_1, C_2, C_3\}$, 其中 C_i 的指标集如下给出:

$$[137\ x\ 8],\ [35\ y\ 1],\ [4\ z\ 1]. \tag{3.4.50}$$

容易验证, PS 中的所有 P_i 关于 CS 的余式都为 0. 因此 CS 是 PS 模因式 F_1, F_2 的一个特征列. 由定理 3.4.17 知

$$\begin{aligned}\mathrm{Zero}(PS) = &\mathrm{Zero}(CS/I_2 * F_1 * F_2) + \mathrm{Zero}(PS + \{I_2\}/F_1 * F_2)\\ &+\mathrm{Zero}(PS + \{F_1\}) + \mathrm{Zero}(PS + \{F_2\}).\end{aligned} \tag{3.4.51}$$

在 (3.4.51) 中, I_2 为 C_2 的初式且是一个指标集为 $[14\ x\ 4]$ 的多项式. C_1 和 C_3 的初式为 $I_1 = (a*b*c+1)^3, I_3 = b*x$. 但它们在 (3.4.51) 中不起作用.

如果我们在过程中不消去任何因子, 那么最终的基列将含有如下多项式:

$$x^4 * (x*b*f - h)^2 * C_1,\ x^2 * C_2,\ 和\ C_3. \tag{3.4.52}$$

PS 中的多项式 P_1, P_3 关于这一基列的余式将不为 0. 因而我们不得不在图表 (S)′ 中继续做下去, 以得到特征列. 计算将会变得很复杂, 以致不能容易算出. 这表明了在特征列的构造中, 如果存在因子的话, 去掉这些因子的重要性.

在最开始时, 我们可以取 P_1 而不是 P_2 作为基列 BS_0 的唯一多项式. 如此继续下去, 在用 (3.4.34) 的步骤中, 消去因式

$$F_3 = x*c*e - k,\ F_4 = x^2 + x*d + g, \tag{3.4.53}$$

则得到一个最终的基列 $CS' = \{C'_1, C'_2, C'_3\}$, 它们的指标集为

$$[137\ x\ 8],\ [79\ y\ 1],\ [4\ z\ 1]. \tag{3.4.54}$$

PS 中所有的 P_i 关于 CS' 的余式都为 0, 所以 CS' 是 PS 模 $F_3 * F_4$ 的一个特征列. 根据定理 3.4.17 有

$$\begin{aligned}\text{Zero}(PS) = &\ \text{Zero}(CS'/I_2' * I_3' * F_3 * F_4) + \text{Zero}(PS + \{I_2'\}/F_3 * F_4) \\ &+\text{Zero}(PS + \{I_3'\}/F_3 * F_4) \\ &+\text{Zero}(PS + \{F_3\}) + \text{Zero}(PS + \{F_4\}).\end{aligned} \tag{3.4.55}$$

在 (3.4.55) 中，I_2', I_3' 分别是 C_2', C_3' 的初式，其中 $I_3' = a * y$, I_2' 是一个指标集为 [36 x 5] 的多项式.

例 3.4.22 (三维空间中的旋转群) 考虑一个旋转 $R = (x_{ij})$, $i, j = 1, 2, 3$, 且满足

$$R^{tr} = R^{-1},\ \det(R) = +1. \tag{3.4.56}$$

确切地说，这一三维空间的旋转群是 $\mathbf{K}^9(x_{ij})$ 中由 Zero(PS) 定义代数簇，这里 $PS = \{P_1, \cdots, P_9, P_{10}\}$, 其中

$$\left.\begin{aligned} P_1 &= x_{11} - (x_{22} * x_{33} - x_{23} * x_{32}), \\ P_2 &= x_{12} + (x_{21} * x_{33} - x_{23} * x_{31}), \\ P_3 &= x_{13} - (x_{21} * x_{32} - x_{22} * x_{31}), \\ P_4 &= x_{21} + (x_{12} * x_{33} - x_{13} * x_{32}), \\ P_5 &= x_{22} - (x_{11} * x_{33} - x_{13} * x_{31}), \\ P_6 &= x_{23} + (x_{11} * x_{32} - x_{12} * x_{31}), \\ P_7 &= x_{31} - (x_{12} * x_{23} - x_{13} * x_{22}), \\ P_8 &= x_{32} + (x_{11} * x_{23} - x_{13} * x_{21}), \\ P_9 &= x_{33} - (x_{11} * x_{22} - x_{12} * x_{21}), \\ P_{10} &= \det(R) - 1. \end{aligned}\right\} \tag{3.4.57}$$

我们选择变量序为

$$x_{11} \prec x_{12} \prec x_{13} \prec x_{21} \prec x_{22} \prec x_{23} \prec x_{31} \prec x_{32} \prec x_{33}. \tag{3.4.58}$$

运用使用了 (3.4.34) 的图表 (S), 在步骤中消去因式 x_{11}, x_{12}, 则得到一个模因式的特征列 $CS = \{C_1, \cdots, C_6\}$, 其中 C_i 如下给出:

$$\left.\begin{aligned} C_1 &= x_{13}^2 + x_{12}^2 + x_{11}^2 - 1, \\ C_2 &= x_{22}^2 * (x_{11}^2 - 1) - 2 * x_{22} * x_{21} * x_{12} * x_{11} \\ &\quad + x_{21}^2 * (x_{12}^2 - 1) - x_{12}^2 - x_{11}^2 + 1, \\ C_3 &= x_{23} * x_{13} + x_{22} * x_{12} + x_{21} * x_{11}, \\ C_4 &= x_{31} - x_{23} * x_{12} + x_{22} * x_{13}, \\ C_5 &= x_{32} + x_{23} * x_{11} - x_{21} * x_{13}, \\ C_6 &= x_{33} - x_{22} * x_{11} + x_{21} * x_{12}. \end{aligned}\right\} \tag{3.4.59}$$

PS 的零点集如下所示:

$$\begin{aligned}\mathrm{Zero}(PS) = &\mathrm{Zero}(CS \ / \ x_{11} * x_{12} * x_{13} * (x_{11}^2 - 1)) \\ &+\mathrm{Zero}(PS + \{x_{13}\} \ / \ x_{11} * x_{12}) \\ &+\mathrm{Zero}(PS + \{x_{11}^2 - 1\} \ / \ x_{11} * x_{12}) \\ &+\mathrm{Zero}(PS + \{x_{11}\}) + \mathrm{Zero}(PS + \{x_{12}\}).\end{aligned} \tag{3.4.60}$$

§3.5 零点分解定理

待研究的问题

本节中的记号和概念，如 $\mathbf{K}$ 等，与前面相同.

在前面的 §3.4 中，我们介绍了多项式集 PS 的特征列的概念，其零点结构与 PS 的零点结构有密切关系，正如定理 3.4.1 中的性质 $(c_1), (c_2)$ 和整序原理 (定理 3.4.8) 所述,

$$\left.\begin{aligned}&\mathrm{Remdr}(PS/CS) = \{0\}, \\ &\mathrm{Zero}(CS/IP) \subset \mathrm{Zero}(PS) \subset \mathrm{Zero}(CS), \\ &\mathrm{Zero}(PS/IP) = \mathrm{Zero}(CS/IP), \\ &\mathrm{Zero}(PS) = \mathrm{Zero}(CS/IP) + \textstyle\bigcup_i \ \mathrm{Zero}(PS + \{I_i\}).\end{aligned}\right\} \tag{3.5.61}$$

在 (3.5.61) 中，CS 是 PS 的一个特征列，IP 是 CS 的初式积，I_i 是 CS 中多项式的初式. $(3.5.61)_4$ 右边的集合 $\mathrm{Zero}(CS/IP)$ 可以认为是 $\mathrm{Zero}(PS)$ 的主要部分. 本节的目的是通过考察 $(3.5.61)_4$ 中的剩余部分来研究以下问题.

问题 D 通过由多项式 PS 确定的升列来确定 PS 的零点结构.

问题 D 的解答将以下面要介绍的零点分解定理的形式给出.

零点分解定理

$(3.5.61)_4$ 右边的集合 $\mathrm{Zero}(CS/IP)$ 通常给出 $\mathrm{Zero}(PS)$ 的主要部分. 如果我们用如前所述的方法处理右边并中的每一个成员，并继续做下去，我们将得到如下的

定理 3.5.1 (零点分解定理 I) 存在一个算法，使得对于给定的多项式集 PS, 可在有限步内得到有限个升列 CS_j, 使得

$$\mathrm{Zero}(PS) = \bigcup_j \ \mathrm{Zero}(CS_j/IP_j), \tag{I}$$

$$\mathrm{Remdr}(PS/CS_j) = \{0\}. \tag{3.5.62}$$

(I) 中的每个 IP_j 为相应升列 CS_j 的初式积. 此外, (3.5.62) 中的每个 CS_j 的序都不高于 PS 的序.

证明 由 $(3.5.61)_2$ 知, 对于 $(3.5.61)_4$ 中并的每个成员, 都有

$$\mathrm{Zero}(PS + \{I_i\}) = \mathrm{Zero}(PS_i), \tag{3.5.63}$$

其中

$$PS_i = PS + CS + \{I_i\}.$$

由于 I_i 关于 CS 是约化的且 CS 的序不高于 PS 的序, 从而由定理 3.3.24 或 3.3.31 有

$$PS \succ PS_i. \tag{3.5.64}$$

于是 $(3.5.61)_4$ 可改写为

$$\mathrm{Zero}(PS) = \mathrm{Zero}(CS/IP) + \bigcup_i \mathrm{Zero}(PS_i). \tag{3.5.65}$$

以同样的方法处理 PS_i, 类似于 (3.5.63), (3.5.64) 和 (3.5.65), 我们得到

$$\left.\begin{array}{l}\mathrm{Zero}(PS_i) = \mathrm{Zero}(CS_i/IP_i) + \bigcup_{i_1} \mathrm{Zero}(PS_{ii_1}),\\ PS_{ii_1} = PS_i + CS_i + \{I_{ii_1}\},\\ PS_i \succ PS_{ii_1}.\end{array}\right\} \tag{3.5.66}$$

在 (3.5.66) 中, CS_i 是 PS_i 的一个特征列, IP_i 是 CS_i 的初式积, I_{ii_1} 是 CS_i 中多项式的初式. 注意到, 由 3.4 节中的整序原理知, CS 的序不高于 PS 的序. 于是, 所有的 PS_i 的序也不高于 PS 的序. 此外, 由于 $PS \subset PS_i$, 作为 CS_i 是 PS_i 的特征列的一个条件的 $(3.5.61)_1$ 表明了 $(3.5.61)_1$ 对 PS 关于 CS_i 也适用, 或者说,

$$\mathrm{Remdr}(PS/CS_i) = \{0\}. \tag{3.5.67}$$

由 (3.5.65) 和 $(3.5.66)_1$ 得到

$$\mathrm{Zero}(PS) = \mathrm{Zero}(CS/IP) + \bigcup_i \mathrm{Zero}(CS_i/IP_i) + \bigcup_{ii_1} \mathrm{Zero}(PS_{ii_1}). \tag{3.5.68}$$

如前所述, 每个 CS_i 和 PS_{ii_1} 的序都不高于 PS_i 的序, 从而也不高于 PS 的序.

我们按前面的方法处理最后一个并集中的每一 PS_i, 如此做下去, 在每一步 k, 我们得到如下形式的等式:

$$\begin{aligned}\mathrm{Zero}(PS) = \mathrm{Zero}(CS/IP) + \textstyle\bigcup_i \mathrm{Zero}(CS_i/IP_i) \\ + \cdots + \textstyle\bigcup_{ii_1\cdots i_k} \mathrm{Zero}(PS_{ii_1\cdots i_k}).\end{aligned} \tag{3.5.69}$$

正如在 (3.5.64) 和 $(3.5.66)_3$ 中一样, 我们有

$$PS \succ PS_i \succ PS_{ii_1} \succ \cdots \succ PS_{ii_1\cdots i_k} \succ \cdots. \tag{3.5.70}$$

根据定理 3.3.26 和 3.3.32, (3.5.70) 中的序列都是有限的. 于是当 k 充分大时, (3.5.69) 中最后一个 $PS_{ii_1\cdots i_k}$ 的并不存在, 于是 (3.5.69) 可以改写为形如 (I) 的等式. 此外, 正如关于 CS 的 $(3.5.61)_1$ 和关于 CS_i 的 (3.5.67), 我们可得到 $\mathrm{Remdr}(PS/CS_{ii_1}) = \{0\}$. 由归纳法知, (3.5.62) 对每个 CS_j 都成立. 更进一步, 由归纳法我们还可得到, (3.5.62) 中的每个 CS_j 的序都不高于 PS 的序. 定理证毕. □

在 §3.4 的定理 3.4.19 中, 以 (3.4.45) 代替 (3.4.32) 或 $(3.5.61)_4$, 按照同样的方法我们得到如下定理.

定理 3.5.2 (零点分解定理 (II)) 存在一个算法, 使得对于给定的多项式集 PS, 可在有限步内计算出有限多个升列 CS_j, 满足

$$\mathrm{Zero}(PS) = \bigcup_k \mathrm{Zero}(CS_k/ISP_k), \tag{II}$$

$$\mathrm{Remdr}(PS/CS_k) = \{0\}. \tag{3.5.71}$$

(II) 中每个 ISP_k 是相应的升列 CS_k 的初式隔离子积. 此外, (3.5.71) 中的每个 CS_k 的序不高于 PS 的序.

定义 3.5.3 上面的定理 3.5.1 或 3.5.2 中给出的升列 CS_j 组成的集合称作 PS 的一个*特征序列*.

下面我们将给出零点分解定理的其他形式. 为此, 和前面几节类似, 我们将引入多项式集的其他偏序关系. 首先, 我们做一些准备.

<u>*多项式对的子消元式序列*</u>

设 $\mathbf{D}$ 为唯一分解整环, A_m, B_n 为 $\mathbf{D}[x]$ 中两个具有如下形式的多项式:

$$\left.\begin{aligned} A_m &= a_m * x^m + \cdots + a_i * x^i + \cdots + a_0,\ a_m \neq 0, \\ B_n &= b_n * x^n + \cdots + b_i * x^i + \cdots + b_0,\ b_n \neq 0, \end{aligned}\right\} \tag{3.5.72}$$

其中 m, n 都大于零.

问题 SE 对任一满足 $0 < g < \min(m,n)$ 的整数 g, 找到系数在 D 中的多项式 $C_{n-g-1}, D_{m-g-1}, E_g$, 使得它们关于 x 的次数分别小于或等于 $n-g-1, m-g-1, g$, 并满足

$$C_{n-g-1} * A_m + D_{m-g-1} * B_n = E_g. \tag{3.5.73}$$

解答 把这些多项式写成具有未定系数 c_i, d_i, e_i 的如下形式:

$$\left.\begin{array}{l} C_{n-g-1} = c_{n-g-1} * x^{n-g-1} + \cdots + c_i * x^i + \cdots + c_0, \\ D_{m-g-1} = d_{m-g-1} * x^{m-g-1} + \cdots + d_i * x^i + \cdots + d_0, \\ E_g = e_g * x^g + \cdots + e_i * x^i + \cdots + e_0. \end{array}\right\} \tag{3.5.74}$$

比较 $(3.5.73)_g$ 中 x 次幂的系数, 从而得到一组方程:

$$\sum_{i=0}^{r} (c_i * a_{r-i} + d_i * b_{r-i}) - e_r = 0, \tag{3.5.75}$$

其中 $r = 0, 1, \cdots, m+n-g-1$. 在 $(3.5.75)_r$ 中, 当 $i > m$ 时, $a_i = 0$; 当 $i > n$ 时, $b_i = 0$; 当 $i > n-g-1$ 时, $c_i = 0$; 当 $i > m-g-1$ 时, $d_i = 0$; 当 $i > g$ 时, $e_i = 0$. (3.5.75) 中的方程个数是 $m+n-g$, 未知数个数关于 c 为 $n-g$ 个, 关于 d 为 $m-g$ 个, 关于 e 为 $g+1$ 个, 所以总共有 $m+n-g+1$ 个. 因为方程组 (3.5.75) 关于这些未定元是齐次线性的, 所以关于 (c,d,e) 总有解. 为明确起见, 我们用以下方法找出一个确切的解.

记号 3.5.4 记 ME_g 为 $m+n-g$ 行 $m+n-g+1$ 列矩阵, 其中的第 r 行是由 $(3.5.75)_r$ 中对应于如下顺序

$$c_{n-g-1}, \cdots, c_0, d_{m-g-1}, \cdots, d_0, e_g, \cdots, e_0 \tag{3.5.76}$$

的 $m+n-g+1$ 个未定元的系数组成.

记号 3.5.5 记 DE_{gi} 为将矩阵 ME_g 的第 i 列去掉后得到的矩阵的行列式和 $(-1)^i$ 的乘积.

定义 3.5.6 A_m, B_n 的第 g *阶子消元式* 定义为 $(3.5.73)_g$ 的确定解 E_g, 它由 (3.5.75) 确定:

$$\begin{aligned}(c_{n-g-1}, \cdots, c_0, d_{m-g-1}, \cdots, d_0, e_g, \cdots, e_0)\\ = (DE_{g1}, \cdots, DE_{g,m+n-g+1}).\end{aligned} \tag{3.5.77}$$

记号 3.5.7 A_m, B_n 的第 g 阶子消元式记为 $E_g(A_m, B_n)$. 在不会产生混淆时, 也简记为 E_g.

注释 3.5.8 根据 Collins 和 Brown 的理论, 多项式 $E_g = E_g(A_m, B_n)$, 其中由 (3.5.77) 给出的 e_i 是 A_m 和 B_n 的子结式 (至多相差一个正负号). 特别地, E_0 是 A_m 和 B_n 的结式 (至多相差一个正负号). 参见 [Col1] 和 [B-T]. 然而, 我们并不需要用到 Collins 和 Brown 提出的整个子结式理论. 对我们来说, 重要的结论由下列命题概括给出. 对这些命题, 我们将给出直接的、不同于 Collins 和 Brown 书中所给的证明.

<u>多项式对的子消元式的性质</u>

由以上定义知,

命题 3.5.9 子消元式 E_g 的系数都是关于 A_m 和 B_n 的系数的确定的多项式.

命题 3.5.10 第 0 阶子消元式 E_0 与 A_m, B_n 的结式至多相差一个正负号.

命题 3.5.11 若 $m \le n$, 则 A_m 和 B_n 的最后的子消元式 E_{m-1} 与 B_n 关于 A_m 的伪余式至多相差一个正负号.

证明 由定义容易验证

$$E_{m-1} = \pm\, a_m^{n-m+1} * B_n + Q * A_m \tag{3.5.78}$$

对于某一多项式 Q. 再由伪余式的定义得到命题的结论. □

由于多项式 E_0 和 A_m, B_n 的结式至多相差一个正负号, E_0 等于零是 A_m, B_n 有一个关于 x 的次数为正的最大公因子的充要条件.

命题 3.5.12 若多项式 A_m 和 B_n 有一个次数为 $f > 0$ 的最大公因子, 则对于 $g < f$, A_m 和 B_n 的子消元式 E_g 都为零.

证明 对 $g < f$, 考虑任一满足 $(3.5.73)_g$ 的 A_m 和 B_n 的子消元式 E_g. 由于 A_m 和 B_n 有最大公因子 F_f, 其次数为 f, 从而 E_g 也有因子 F_f. 由于 E_g 的次数 $\le g$, 所以当 $g < f$ 时, 只可能有 $E_g = 0$. □

命题 3.5.13 若 $E_0 = 0$, 即 A_m, B_n 有一个次数 $f > 0$ 的最大公因子, 则这个最大公因子和 A_m, B_n 的第一个非零子消元式 E_g 至多相差 $\mathbf{D}$ 中的一个非零常量.

证明 设 A_m 和 B_n 的最大公因子为 F_f, 其关于 x 的次数为 $f > 0$. 设

$$A_m = A'_{m-f} * F_f, \quad B_n = B'_{n-f} * F_f, \tag{3.5.79}$$

其中 A'_{m-f} 和 B'_{n-f} 分别是次数为 $m-f$ 和 $n-f$ 的多项式. 可能出现最大公因子 F_f 的次数为 $\min(m,n)$, 从而, A_m, B_n 中的某一个多项式是另一个多项式的本原部分的倍数. 不考虑这种情形, 多项式 A'_{m-f} 和 B'_{n-f} 关于 x 的次数均为正, 而且没有正次数的公因子. 记 A'_{m-f} 和 B'_{n-f} 的零阶子消元式为 E'_0, 从而存在多项式 C'_{n-f-1} 和 D'_{m-f-1}, 它们的次数分别 $\le n-f-1$ 和 $m-f-1$, 使得

$$C'_{n-f-1} * A'_{m-f} + D'_{m-f-1} * B'_{n-f} = E'_0. \tag{3.5.80}$$

由于 E'_0 和 A'_{m-f}, B'_{n-f} 的结式至多相差一个正负号, 且 A'_{m-f} 和 B'_{n-f} 没有次数为正的公因子, 所以 $E'_0 \neq 0$. 在 (3.5.80) 的两侧乘以 F_f, 我们得到

$$C'_{n-f-1} * A_m + D'_{m-f-1} * B_n = E'_0 * F_f. \tag{3.5.81}$$

另一方面, 对 $g=f$, 由 $(3.5.73)_g$ 有

$$C_{n-f-1} * A_m + D_{m-f-1} * B_n = E_f. \tag{3.5.82}$$

我们知道 E_f 关于 x 的次数恰为 f. 证明参见如 [Bo] 或 [Ak] 的第 239 页. 消去方程 (3.5.81) 和 (3.5.82) 右边中的最高次项, 则得到一个如下形式的方程:

$$C''_{n-f-1} * A_m + D''_{m-f-1} * B_n = G,$$

其中 G 为次数小于 f 的多项式. 由命题 3.5.12 知, G 必为 0, 从而 E_f 和 $E'_0 * F_f$ 仅相差 $\mathbf{D}$ 中的一个非零常量. 命题证毕. □

<u>多项式对的指数和消元式</u>

现考虑 $E_0 \neq 0$ 的情形.

A_m 和 B_n 的子消元式 E_0 由 $(3.5.73)_g$ 给出, 其中 $g=0$, 即

$$C_{n-1} * A_m + D_{m-1} * B_n = E_0. \tag{3.5.83}$$

此时, A_m 和 B_n 没有正次数的公因子. 因此在 $(3.5.73)_g$ 中, $E_g = 0$ 表明 $C_{n-g-1} = 0$ 和 $D_{m-g-1} = 0$.

若对于某个 $g > 0$, 多项式 E_g 的次数为零, 且为 $\mathbf{D}$ 中的非零常量, 则在 (3.5.83) 和 $(3.5.73)_g$ 中消去 E_0, E_g 后得到一个如下形式的方程:

$$(E_g * C_{n-1} - E_0 * C_{n-g-1}) * A_m + (E_g * D_{m-1} - E_0 * D_{m-g-1}) * B_n = 0.$$

在前面的讨论中, 或者 A_m 和 B_n 的系数都为零, 或者方程 (3.5.83) 和 $(3.5.73)_g$ 相互成比例. 这样, 只有 $deg(E_g)>0$ 的子消元式 E_g, 特别是下标 g 最小的那个 E_g, 才是我们关心的. 我们给出如下的

定义 3.5.14 多项式 E_g 关于 x 的次数为正的最小的整数 g, 如果它存在的话.

定义 3.5.15 若 $E_0 \neq 0$, A_m 和 B_n 的消元式定义为子消元式 E_e, 如果 A_m 和 B_n 的指数存在并等于 e.

以上是子结式理论中我们所需要的部分.

与多项式集合相关的整数集合

定义 3.5.16 多项式集 PS 的 *类集* 定义为 PS 中多项式的不同的正的类组成的集合, 并按递减顺序排列为

$$(c_1, \cdots, c_r), \quad 其中\ c_1 > c_2 > \cdots > c_r > 0. \tag{3.5.84}$$

定义 3.5.17 多项式集 PS 的 *次数集* 定义为集合

$$(d_1, \cdots, d_r), \tag{3.5.85}$$

其中 d_i 是 PS 中所有类为 c_i 的多项式的次数中最小的一个, 这里 c_i 属于类集 (3.5.84).

定义 3.5.18 多项式集 PS 的 *多项式个数集* 定义为集合

$$(n_1, \cdots, n_r), \tag{3.5.86}$$

其中 n_i 是 PS 中类为 c_i 的多项式的个数, 这里 c_i 属于类集 (3.5.84).

记号 3.5.19 $cs(PS) :=PS$ 的类集,

$ds(PS) :=PS$ 的次数集,

$pns(PS) :=PS$ 的个数集.

注释 3.5.20 以上集合都有可能为空, 即 PS 仅由 $\mathbf{K}$ 中的非零元素组成. 此时, $\mathrm{Zero}(PS)$ 也为空. 此外, 若 PS 中有一个非零常量, 则 $\mathrm{Zero}(PS)$ 为空集.

定义 3.5.21 对于类集非空的多项式集 PS, PS 的 *主导类* 定义为使得对应类为 c 的多项式的个数大于 1 的最大的类 c, 如果这样的类存在的话; 否则, PS 的主导类定义为零.

定义 3.5.22 对于一个类集非空的多项式集 PS, PS 的 *主导次数* 定义为 PS 中的主导类中的多项式的次数中的最小者, 如果存在的话; 否则不定义.

<u>多项式集的一个偏序</u>

定义 3.5.23　称多项式集 PS高于多项式集 PS' 或 PS' 低于PS, 如果下列条件 (a)~(d) 之一成立：

(a) PS 的类集 $(c_1,\cdots,c_r)$ 和 PS' 的类集 $(c_1',\cdots,c_s')$ 均非空，且对于使得 $c_k \neq c_k'$ 的最小下标 k, 有 $c_k > c_k'$.

(b) PS 和 PS' 的类集均非空，它们的前 k 个类相同，但它们的次数集里使得 $d_j \neq d_j'$ 的最小下标 $j = k$ 且 $d_k > d_k'$.

(c) PS 和 PS' 的类集、次数集均非空，它们的前 k 个类和次数都相同，但它们的多项式个数集里使得 $n_j \neq n_j'$ 的最小下标 $j = k$ 且 $n_k > n_k'$.

(d) PS 的类集非空，而 PS' 的类集是空集.

定义 3.5.24　称 PS 和 PS' 是不可比较的, 如果 PS 和 PS' 中的任何一个都不高于另一个.

记号 3.5.25　用 $PS > PS'$ 或 $PS' < PS$ 记 PS 高于 PS' 或 PS' 低于 PS.

记号 3.5.26　用 $PS <> PS'$ 记 PS,PS' 不可比较.

以下引理可由上述定义直接得出.

引理 3.5.27　设 TS 是一个三角列，PS' 是在 TS 中添加一个关于 TS 约化的多项式得到的多项式集. 若 TS 和 PS' 的类集相同，则 $PS' < TS$.

引理 3.5.28　序不断递减的多项式序列是有限的.

证明　略.　□

<u>替换法则和多项式的降序</u>

我们的另一种特征列方法在于利用下面给出的替换法则用一些序更低的多项式集来代替 PS. 自然地，我们可假设 PS 的类集非空.

替换法则 1　假设 PS 中的某个类为 $c > 0$ 的多项式 P 可以分解为 $P = P_1 * P_2$, 其中 P_1, P_2 的类均为 c. 于是我们可作如下替换：

$$\left.\begin{aligned} &PS \longrightarrow PS_1 + PS_2, \\ &\text{其中} \\ &PS_1 = PS \setminus \{P\} + \{P_1\}, \\ &PS_2 = PS \setminus \{P\} + \{P_2\}. \end{aligned}\right\} \tag{3.5.87}$$

显然，

$$\mathrm{Zero}(PS) = \mathrm{Zero}(PS_1) + \mathrm{Zero}(PS_2), \tag{3.5.88}$$

且

$$PS_1 < \text{或} <> PS,\ PS_2 < \text{或} <> PS. \tag{3.5.89}$$

替换法则2 假设 PS 的主导类 $c>0$. 设 A 为一个类为 c, 次数为主导次数的多项式, B 是 PS 中的类为 c 的另一多项式. 设 E_0 为 A 和 B 关于 x_c 的零阶子消元式或结式 (仅只差一个正负号). 分几种不同的情形:

情形 1: $E_0=0$.

此时, A 和 B 有最大公因子 F, 其类为 c, 次数 $f>0$. 作如下替换:

$$\left.\begin{aligned} &PS \longrightarrow PS_1+PS_2, \\ &\text{其中} \\ &PS_1 = PS\setminus\{A,B\}+\{F\}, \\ &PS_2 = PS\setminus\{A,B\}+\{A/F,B/F\}. \end{aligned}\right\} \tag{3.5.90}$$

显然, (3.5.88), (3.5.89) 成立.

情形 2: $E_0\neq 0$, 多项式对 (A,B) 的指数存在且 >0.

设该指数为 e. 于是消元式 E_e 的类为 c, 它关于 x_c 的次数为正且小于 A 的次数. 现作如下替换:

$$PS \longrightarrow PS_1 = PS\setminus\{A,B\}+\{E_0,E_e\}.$$

显然有

$$\mathrm{Zero}(PS)\subset \mathrm{Zero}(PS_1), \tag{3.5.91}$$

且

$$PS_1 < PS. \tag{3.5.92}$$

情形 3: $E_0\neq 0$, 多项式对 (A,B) 的指数不存在. 显然, 这即为 A 关于 x_c 的次数为 1 的情形.

此时作如下代换:

$$PS \longrightarrow PS_1 = PS\setminus\{B\}+\{E_0\}.$$

显然, (3.5.91) 和 (3.5.92) 在这一情况下仍成立.

注释 3.5.29 在这些替换规则中, 类集中类的个数不会减少. 类的个数的增加只可能出现在规则 2 的情形 2 或 3 中. 此时零阶子消元式 E_0 的类为正且不在原类集中.

替换规则 3 考虑任意三角列 TS 和多项式集 PS. 作 PS 中的多项式关于 TS 的余式. 假设这些余式中有非零多项式. 此时, 将所有这些非零余式加到 TS 中得到一个多项式集 PS'. 于是由引理 3.5.1 知, 若类集不变, 则

$$PS' < TS,$$

或

$$\mathrm{Zero}(TS + PS) \subset \mathrm{Zero}(PS'). \tag{3.5.93}$$

注释 3.5.30 在替换规则 3 中, 若类集变化, 则类集中的类的个数将增加.

利用替换规则进行零点分解的另一种步骤

对给定的多项式集 PS 和其后得到的多项式集尽可能地应用替换规则 1 和 2, 最终我们将得到一组三角列 TS_i, 使得

$$\mathrm{Zero}(PS) \subset \bigcup_i \mathrm{Zero}(TS_i). \tag{T}$$

由这一包含关系显然有

$$\mathrm{Zero}(PS) = \bigcup_i \mathrm{Zero}(TS_i + PS). \tag{T$'$}$$

对分解 (T)$'$ 中出现的每个 $TS_i + PS$ 运用替换规则 3, 并尽可能地利用替换规则 1~3 重复这一过程. 由于类的个数由 n 限制, 我们最终将得到一个与 (T) 形式相同的分解, 同时该分解还满足如下性质:

$$\mathrm{Remdr}(PS/TS_i) = \{0\}. \tag{3.5.94}$$

对 (T) 中的每一个满足 (3.5.94) 的三角列 TS_i, 把 $\mathrm{Zero}(TS_i)$ 替换为

$$\mathrm{Zero}(TS_i) = \mathrm{Zero}(TS_i/J_i) + \bigcup_j \mathrm{Zero}(TS_{ij} + \{I_{ij}\}).$$

在这一表达式中, TS_{ij} 是将 TS_i 中多项式的首项去掉后得到的多项式集, I_{ij} 是第 j 个多项式的初式, J_i 是 TS_i 中所有这样的多项式的初式积. 由引理 3.5.1 知, 所有的集合 $TS_{ij} + \{I_{ij}\}$ 的序都低于 TS_i, 因此我们可以尽可能地重复这一步骤. 根据引理 3.5.2, 我们最后将得到如下形式的关系式:

$$\mathrm{Zero}(PS) \subset \bigcup_k \mathrm{Zero}(TS_k/IP_k),$$

其中 IP_k 是 TS_k 的初式积，且 (3.5.94) 对每个 TS_k 都成立. 于是易知，上述包含关系实际上是一个等式. 于是，上述讨论给出了一个可获得如下形式分解的算法:

$$\mathrm{Zero}(PS) = \bigcup_k \mathrm{Zero}(TS_k/IP_k), \tag{III}$$

其中每个 TS_k 是一个满足 (3.5.94) 的三角列,IP_k 是 TS_k 的初式积. 如果 TS_k 中某个多项式的初式关于该多项式之前的多项式组成的部分升列不约化，则对该多项式运用替换规则 3. 这样，分解 (III) 终将化成一个形如 (I) 的分解. 这样就给出了得到分解 (I) 的另一种算法.

示例

例 3.5.31 考虑例 3.4.15 和 3.4.20.

首先考虑 (3.4.42), 其中没有任何非平凡因子在步骤中被消去. 为了得到定理 3.5.1 中的分解，我们必须确定 $\mathrm{Zero}(PS+\{I_1\})$. 利用特征列算法，我们得到 $PS+\{I_1\}$ 的一个特征列:

$$CS_1 = \{C_{11}, C_{12}, C_{13}\}, \tag{3.5.95}$$

其中

$$\left.\begin{aligned} C_{11} &= (z-1)^2*(z+1)*(z-5),\\ C_{12} &= x*z*(z+1)*(z-5),\\ C_{13} &= -y-x^2+x*z+x-z. \end{aligned}\right\} \tag{3.5.96}$$

于是,

$$\mathrm{Zero}(PS+\{I_1\}) = \mathrm{Zero}(CS_1/I_{12}) + \mathrm{Zero}(PS+\{I_1, I_{12}\}), \tag{3.5.97}$$

其中

$$I_{12} = z*(z+1)*(z-5) \tag{3.5.98}$$

是 C_{12} 的初式.

我们得到 $(PS+\{I_1, I_{12}\})$ 的特征列为

$$CS_2 = \{C_{21}, C_{22}, C_{23}\}, \tag{3.5.99}$$

其中,

$$\left.\begin{aligned} C_{21} &= (z+1)*(z-5),\\ C_{22} &= x*(x*(z-2)-2*z+1),\\ C_{23} &= -y-x^2+x*z+x-z. \end{aligned}\right\} \tag{3.5.100}$$

此时，显然有

$$\mathrm{Zero}(PS+\{I_1,I_{12}\})=\mathrm{Zero}(CS_2). \tag{3.5.101}$$

结合 (3.4.42), (3.5.97), (3.5.101), 我们得到所求的分解:

$$\mathrm{Zero}(PS)=\mathrm{Zero}(CS/I_1)+\mathrm{Zero}(CS_1/I_{12})+\mathrm{Zero}(CS_2). \tag{3.5.102}$$

(3.5.102) 右边的零点集分别如下给出:

$$\left.\begin{array}{l}(z,x,y)=(z,0,-z),\ \text{其中}\ z\neq 1,-1,5\\(z,x,y)=(1,0,-1)\\(z,x,y)=(-1,1,0),\ (-1,0,1),\ (5,3,4)\ \text{或}\ (5,0,-5)\end{array}\right\} \tag{3.5.103}$$

因此, PS 的零点集由空间 $\mathbf{K}^3(z,x,y)$ 中的一条直线 $x=0,y+z=0$ 和两个孤立点 $(-1,1,0),(5,3,4)$ 组成.

现考虑在步骤中消去因子 x 后得到的 (3.4.47). 对 $PS+\{x\}$, 容易得到它的一个特征列为

$$CS_1'=\{C_{11}',C_{12}'\}, \tag{3.5.104}$$

其中

$$\begin{aligned}C_{11}'&=x,\\C_{12}'&=y+z.\end{aligned} \tag{3.5.105}$$

于是有

$$\mathrm{Zero}(PS+\{x\})=\mathrm{Zero}(CS_1'). \tag{3.5.106}$$

容易看出

$$\begin{aligned}&\mathrm{Zero}(CS'\ /\ x*(z-2))=\mathrm{Zero}(CS'),\\&\mathrm{Zero}(PS+\{z-2\}/x)=\emptyset.\end{aligned}$$

结合 (3.4.46), (3.4.50), 我们得到完全的分解:

$$\mathrm{Zero}(PS)=\mathrm{Zero}(CS')+\mathrm{Zero}(CS_1'). \tag{3.5.107}$$

容易看出，其零点集由一条直线和两个孤立点组成.

例 3.5.32 仍考虑 Czapor 和 Geddes 的例 3.4.21. 注意到 (3.4.48) 中的 a,b 等都看作独立的参数. 因而在公式 (3.4.51) 中, 有

$$\begin{gathered}\mathrm{Zero}(PS+\{I_2\}/F_1*F_2)=\emptyset,\ \mathrm{Zero}(PS+\{F_1\})=\emptyset,\\ \mathrm{Zero}(PS+\{F_2\})=\emptyset.\end{gathered} \tag{3.5.108}$$

事实上, 最后两个等式可以直接验证, 因为它们将导出关于独立参数 a,b 等的非零多项式, 这些参数可看作是非零的. 对于 (3.5.108) 中的第一个等式, 注意到由 (3.4.52) 有

$$x^4*(x*b*f-h)*C_1=0 \mid \mathrm{Zero}(PS),$$

其中 C_1 是指标集为 $[137\ x\ 8]$ 的多项式且不可约. 另一方面, I_2 是一个指标集为 $[14\ x\ 4]$ 的多项式, 其关于 x 的次数为 4. 于是, C_1 和 I_2 关于 x 的结式是一个关于 a,b 等独立参数的非零多项式, 从而非零. 故 I_2 和 C_1 在簇 $\mathrm{Zero}(PS)$ 上不能同时为零. 显然, I_2 和 x 或和 $x*b*f-h$ 在簇 $\mathrm{Zero}(PS)$ 上不能同时为零. 于是有 $\mathrm{Zero}(PS+\{I_2\})=\emptyset$, 进而有 (3.5.108) 的第一个等式. 同理, 我们有

$$\mathrm{Zero}(CS/I_2*F_1*F_2)=\mathrm{Zero}(CS), \tag{3.5.109}$$

因为 I_2,F_1,F_2 关于 x 的次数都小于 C_1 的次数, 从而都和 C_1 有关于 a,b 等的非零结式. 于是由 (3.5.108), (3.5.109), (3.4.51) 最终变为

$$\mathrm{Zero}(PS)=\mathrm{Zero}(CS). \tag{3.5.110}$$

这样就在关于独立参数 a,b 等的一般情形下完全确定了 $\mathrm{Zero}(PS)$. 注意到, 上面用到的确定零点集的推导是一种很一般的方法, 因次可以很方便地应用于各种不同的情形.

最后注意到, 我们还可以利用零点分解 (III) 来确定本例中的 $\mathrm{Zero}(PS)$, 并得到同样的结果. 这里不再赘述.

例 3.5.33 仍考虑例 3.4.22, 其中 PS 由 (3.4.57) 给出, $\mathrm{Zero}(PS)$ 由 (3.4.60) 给出. 注意到方程 $C_1=x_{13}^2+x_{12}^2+x_{11}^2-1=0$. 当 $\mathbf{K}=\mathbf{R}$, 有

$$\mathrm{Zero}_{\mathbf{R}}(PS+\{x_{11}^2-1\}\ /\ x_{11}*x_{12})=\emptyset, \tag{3.5.111}$$

$$\mathrm{Zero}_{\mathbf{R}}(CS\ /\ x_{11}*x_{12}*x_{13}*(x_{11}^2-1))=\mathrm{Zero}_{\mathbf{R}}(CS\ /\ x_{11}*x_{12}*x_{13}). \tag{3.5.112}$$

考虑到 (3.5.111) 和 (3.5.112), 在 $\mathbf{K}=\mathbf{R}$ 时, (3.4.60) 变为

$$\mathrm{Zero}_{\mathbf{R}}(PS)=\mathrm{Zero}_{\mathbf{R}}(CS\ /\ x_{11}*x_{12}*x_{13})+\bigcup_{i=1,2,3}\mathrm{Zero}_{\mathbf{R}}(PS+\{x_{1i}\}). \tag{3.5.113}$$

最后三个零点集特征相同, 都可用上述一般方法处理, 这里不再叙述.

§3.6　簇分解定理

记号 3.6.1　$\mathbf{K}, X=(x_1,\cdots,x_n)$ 等记号与前面相同.

<u>*不可约升列*</u>

考虑一个按升序排列的非平凡升列:

$$AS:\quad A_1,A_2,\cdots,A_r, \tag{3.6.114}$$

其中 $i=1,\cdots,r$.

$$0<c_1<c_2<\cdots<c_r, \tag{3.6.115}$$

$$A_i=I_{i,0}*x_{c_i}^{d_i}+\cdots+I_{i,j}*x_{c_i}^{d_i-j}+\cdots+I_{i,d_i}, \tag{3.6.116}$$

$$I_{ij}\in\mathbf{K}[X_{c_i-1}],\ I_{i,0}\neq 0. \tag{3.6.117}$$

定义 3.6.2　由 (3.6.114) 的前 k 个多项式组成的升列

$$AS_k:\quad A_1,A_2,\cdots,A_k,$$

称作 AS 的 *k 级部分升列*.

定义 3.6.3　(3.6.114) 中的升列 AS 称为 k 级 *不可约的*$(1\leq k\leq r)$, 如果下列条件成立:

对 $k=1$, A_1 在 $\mathbf{K}[X_{c_1}]$ 中不可约.

对 $k>1$, AS 为 $(k-1)$ 级不可约的. 此外, 令 $\mathbf{K}_{c_k-1}$ 为 $\mathbf{K}$ 的以如下方式得到的扩域: 若 $1<j<c_k$, 且 j 不等于任何 c_i, 则将 x_j 作为独立的超越元添加到 $\mathbf{K}$ 上; 将 $x_{c_i}(i<k)$ 通过不可约方程 $A_i=0$, 其中 $i=1,\cdots,k-1$, 逐个地添加到 $\mathbf{K}$ 上. 因此, A_k 作为 x_{c_k} 的多项式在 $\mathbf{K}[X_{c_k}]$ 中是本原的, 且在扩域 $\mathbf{K}(X_{c_k-1})$ 上是不可约的, 即不存在两个类为 c_k 的多项式 $F_{k1},F_{k2}\in\mathbf{K}[X_{c_k}]$ 以及多项式 $I\in\mathbf{K}[X_{c_k-1}]$, 使得 $I*A_k\equiv F_{k1}*F_{k2}\ \mathrm{mod}_{\mathbf{K}}\ AS_{k-1}$.

定义 3.6.4 (3.6.114) 中的升列 AS 称作是 不可约的, 如果它是 r 级不可约的.

例 3.6.5 考虑升列 AS : A_1, A_2, 其中

$$A_1 = x_2^2 + x_1, \ A_2 = x_3^2 + x_1.$$

显然,AS 是 1 级不可约的, 但不是 2 级不可约的, 因为 $A_2 \equiv (x_3 + x_2) * (x_3 - x_2) + A_1$,从而 $A_2 \equiv (x_3 + x_2) * (x_3 - x_2) \bmod_{\mathbf{K}} A_1$.

定理 3.6.6 设 AS 为 (3.6.114)~(3.6.117) 中给出的不可约升列. 令 $E_i = \frac{A_i}{I_{i0}}$, 则 $ES = \{E_1, \cdots, E_r\}$ 是 $\mathbf{K}^n$ 中满足所有 $A_i = 0$ 的扩张点 $\Xi = (\xi_1, \cdots, \xi_n)$ 的定义多项式集. 若 P 是一个关于 AS 约化的非零多项式, 则

$$P(\Xi) \neq 0.$$

特别地, 对于 AS 中任一多项式 A_i 的初式 I_{i0}, 我们有

$$I_{i0}(\Xi) \neq 0.$$

证明 由定义, 定理的第一部分是显然的. 为了证明定理的第二部分, 设 P 为一个关于 AS 约化的多项式. 我们只需证明由 $P(\Xi) = 0$ 可推出 $P \equiv 0$ 即可. 对 P 的类 c 施用归纳法. 将类为 c 的 P 写成典范形式:

$$P = I_0 * x_c^d + \cdots + I_d,$$

其中系数 $I_k \in \mathbf{K}[X_{c-1}]$. 由于 $P(\Xi) = 0$ 且 AS 是不可约的, 从而有 $I_k = 0$, 如果 c 不等于任何 c_i. 另一方面, 若 c 等于某个 c_i, 则由 P 关于 AS 约化知 $d < d_i$, 从而又有: 所有的 $I_k = 0$, 对 $X = \Xi$. 由归纳法知所有的 $I_k \equiv 0$, 从而 $P \equiv 0$. 由于上述推理对 $c \leq c_1$ 也成立, 定理证毕. □

定理 3.6.7 一个不可约升列唯一地确定 $\mathbf{K}^n$ 中共轭扩张点的定义多项式集. 反过来, $\mathbf{K}^n$ 中的任一扩张点的定义多项式集可确定那些确定了给定多项式集的不可约升列.

证明 设不可约升列 AS 如 (3.6.114)~(3.6.117) 所给出. 令 $E_i = A_i/I_{i0}$, $i = 1, \cdots, r$. 于是 E_i 在相应的扩域中是不可约的, 且确定了一个共轭扩张点集合. 反过来, 假设扩张点的定义多项式 E_i 如 (3.1.1) 所给出. 消去方程 $E_i = 0$ 的分母, 我们将依次得到一组多项式方程 $A_i = 0$. 于是 $AS = \{A_1, \cdots, A_r\}$ 是一个按升序排列的不可约升列. □

例 3.6.8　考虑升列 $AS = \{A_1, A_2\}$, 其中

$$A_1 = x_2^2 - x_1,\ A_2 = x_1 * x_3 - x_2^3.$$

它是一个不可约升列，并确定了一个扩张点 Ξ, 其定义多项式为

$$E_1 = x_2^2 - x_1,\ E_2 = x_3 - x_2.$$

点 Ξ 也同样可以由不可约升列 $AS' = \{A_1', A_2'\}$ 确定，其中

$$A_1' = A_1,\ A_2' = x_2 * x_3 - x_1.$$

注释 3.6.9　比较命题 3.1.19 和 3.1.20, 从例 3.6.5, 3.6.8 可看出，不可约升列的概念尽管本质上等价于扩张点的概念，但在表示上要比后者更为灵活. 以后，我们将遇到更复杂的不可约升列.

注释 3.6.10　判定 (3.6.114) 中的升列是否不可约并不容易，因为它牵涉到代数扩域中多项式的分解问题. 我们将在第 4 章的 §4.5 节中处理这一分解问题.

定义 3.6.11　任一确定 $\mathbf{K}^n$ 中扩张点 Ξ 的不可约升列 AS 称为 Ξ 的一个*定义升列*.

<u>扩张点的特定化</u>

定理 3.6.12　设 $\mathbf{K}^n$ 中的扩张点 $\Xi = (\xi_1, \cdots, \xi_n)$ 的定义升列为 AS, 则对于任意多项式 P, 有

$$P(\Xi) = 0 \iff \mathrm{Remdr}(P/AS) = 0. \tag{3.6.118}$$

证明　设 AS 由 (3.6.114) 给出，且 $A_i(\Xi) = 0$. 根据余式公式 (3.3.24), 对任一多项式 P 有

$$I_P * P = \sum_i Q_i * A_i + R, \tag{3.6.119}$$

其中 I_P 是 A_i 的初式的某一幂积, R 为余式 $\mathrm{Remdr}(P/AS)$. 由定理 3.6.6 知, $I_P(\Xi) \neq 0$. 于是，由 (3.6.119) 有

$$P(\Xi) = 0 \iff R(\Xi) = 0.$$

由于 R 关于 AS 约化，再由定理 3.6.6 有

$$R(\Xi) = 0 \iff R = 0.$$

这样，我们得到 (3.6.118), 定理证毕.　　□

定理 3.6.13 设 Ξ 和 Ξ' 为 $\mathbf{K}^n$ 中的两个扩张点，它们的定义升列分别为 AS 和 AS'. 若 Ξ' 是 Ξ 在 $\mathbf{K}$ 上的特定化，则

$$\text{Remdr}(AS/AS') = 0. \tag{3.6.120}$$

反过来，若 (3.6.120) 成立且

$$I_{i0}(\Xi') \neq 0 \text{ 或 } \text{Remdr}(I_{i0}/AS') \neq 0, \tag{3.6.121}$$

对 AS 中的任一多项式 A_i, 其中 $init(A_i) = I_{i0}$, 则 Ξ' 是 Ξ 的一个特定化.

证明 设 AS 由 (3.6.114) 给出.

首先假设 Ξ' 是 Ξ 在 $\mathbf{K}$ 上的一个特定化. 由于 $A_i(\Xi) = 0$, 我们有 $A_i(\Xi') = 0$. 由定理 3.6.12 知, $\text{Remdr}(A_i/AS') = 0$, 从而 (3.6.120) 成立.

反过来，设 (3.6.120) 成立. 由定理 3.6.12 有 $A_i(\Xi') = 0$. 考虑任一满足 $P(\Xi) = 0$ 的多项式 P, 再由定理 3.6.12 知，在 (3.6.119) 中，$R \equiv 0$. 若 (3.6.121) 成立，则 $I_P(\Xi') \neq 0$, 从而由 (3.6.119) 可推出 $P(\Xi') = 0$. 因此，Ξ' 是 Ξ 在 $\mathbf{K}$ 上的一个特定化. □

注释 3.6.14 以上定理部分解决了 §3.1 中的问题 S.

<u>与不可约升列相关的代数簇</u>

定义 3.6.15 对一个不可约升列 IRR, 设 Ξ 是任一以 IRR 为定义升列的扩张点. 于是代数簇 $\text{Spec}_{\mathbf{K}}(\Xi)$ 只取决于 IRR. 我们称它为与 IRR相关的代数簇.

记号 3.6.16 对一个不可约升列 IRR, 记 $\text{Var}[IRR]$ 为与 IRR 相关的代数簇.

由定义 3.6.15 知，对于一个定义了扩张点 Ξ 的不可约升列 IRR,

$$\text{Var}[IRR] = \text{Spec}_{\mathbf{K}}(\Xi). \tag{3.6.122}$$

定理 3.6.17 对于不可约升列 IRR, 我们有

$$\text{Var}[IRR] \subset \text{Zero}(IRR). \tag{3.6.123}$$

证明 设 IRR 的多项式由 (3.6.114) 给出. 对于 $\text{Var}[IRR]$ 的母点 Ξ, 我们有 $A_i(\Xi) = 0$. 由于 $\text{Var}[IRR]$ 中的任一点 Ξ' 都是 Ξ 的一个特定化，所以 $A_i(\Xi') = 0$. 因此, $\Xi' \in \text{Zero}(IRR)$. (3.6.123) 成立. □

定义 3.6.18 设 IRR 为一个不可约升列， IP 为它的初式积. 将 $\text{Zero}(IRR/IP)$ 的一个零点称作不可约升列 IRR 的一个 *正则零点*.

定理 3.6.19 一个不可约升列 IRR 的任一正则零点都是簇 Var[IRR] 的一个点，即

$$\mathrm{Zero}(IRR/IP) \subset \mathrm{Var}[IRR]. \tag{3.6.124}$$

证明 设 Ξ 为 Var[IRR] 的一个母点. 考虑满足 $P(\Xi)=0$ 的任一多项式 P. 由定理 3.6.12 知，$\mathrm{Remdr}(P/IRR)=0$. 于是由余式公式，存在某个 IRR 中的多项式初式积 I_P 的幂积，使得 $I_P * P$ 是 IRR 中多项式的以多项式为系数的线性组合. 设 Ξ' 为 IRR 的一个正则零点，从而 $I_P(\Xi') \neq 0$. 于是上述的余式公式给出 $P(\Xi')=0$. 由此有，Ξ' 是 Ξ 在 $\mathbf{K}$ 上的一个特定化，因而属于 Var[IRR]. □

注释 3.6.20 一般而言，

$$\mathrm{Var}[IRR] \neq \mathrm{Zero}(IRR). \tag{3.6.125}$$

鉴于 (3.6.123) 和 (3.6.125)，为了避免混淆我们用方括号 [ ] 而不是圆括号 ( ) 来表示相关的簇. 参见下面的例 3.6.32.

<u>与不可约升列相关的理想</u>

定理 3.6.21 设 IRR 为一个不可约升列，则所有关于 IRR 余式为零的多项式构成一个素理想.

证明 由定理 3.6.12 知，关于 IRR 余式为零的多项式 P 具有性质：$P(\Xi)=0$，其中 Ξ 为簇 Var[IRR] 的一个母点. 由这一性质可直接推出，所有这样的多项式构成一个理想，事实上，为一个素理想. □

记号 3.6.22 定理 3.6.21 中由 IRR 确定的理想记作 Ideal[IRR].

定义 3.6.23 理想 Ideal[IRR] 称为与不可约升列 *IRR相关的理想*.

注释 3.6.24 设 Ideal(PS) 是一个以多项式集 PS 为基的理想，则有

$$\mathrm{Ideal}[IRR] \supset \mathrm{Ideal}(IRR). \tag{3.6.126}$$

但一般说来，

$$\mathrm{Ideal}[IRR] \neq \mathrm{Ideal}(IRR). \tag{3.6.127}$$

鉴于 (3.6.126) 和 (3.6.127)，为了避免混淆我们用方括号 [ ] 而不是圆括号 ( ) 来表示相关的理想. 参见下面的例 3.6.32.

<u>Var[IRR] 或 Ideal[IRR] 的有限基</u>

下面的定理 3.6.25 和 3.6.27 将推迟到以后几章加以证明.

定理 3.6.25 根据周炜良关于周形式的理论，存在一个算法，使得对于任一不可约升列 IRR, 将在有限步内给出 $\mathrm{Var}[IRR]$ 或 $\mathrm{Ideal}[IRR]$ 的一组有限基 CB, 且 CB 由 IRR 直接确定，使得

$$\begin{aligned}\mathrm{Var}[IRR] &= \mathrm{Zero}(CB),\\ \mathrm{Ideal}[IRR] &= \mathrm{Ideal}(CB).\end{aligned} \tag{3.6.128}$$

定义 3.6.26 定理 3.6.25 或 (3.6.128) 中的基 CB 称为理想 $\mathrm{Ideal}[IRR]$ 或簇 $\mathrm{Var}[IRR]$ 的 周基.

定理 3.6.27 设 $V = \mathrm{Var}[IRR]$,$V' = \mathrm{Var}[IRR']$ 分别为与不可约升列 IRR 和 IRR' 相关的代数簇，CB 为 $\mathrm{Var}[IRR]$ 或 $\mathrm{Ideal}[IRR]$ 的周基，则 V' 为 V 的一个子簇当且仅当

$$\mathrm{Remdr}(CB/IRR') = 0. \tag{3.6.129}$$

证明 由基的定义有

$$\mathrm{Var}[IRR] = \mathrm{Zero}(CB).$$

设 Ξ' 为 V' 的一个母点，则由定理 3.6.12 知，(3.6.129) 等价于

$$P(\Xi') = 0, \quad \text{对所有的 } P \in CB,$$

或

$$P = 0 \mid V', \quad \text{对所有的 } P \in CB,$$

或

$$V' \subset \mathrm{Zero}(CB).$$

由此 (3.6.129) 等价于 $V' \subset V$. □

注释 3.6.28 定理 3.6.27 对 3.1 节中的问题 S 作了完全的解答.

<u>簇分解定理</u>

定理 3.6.29 存在一个算法，使得对任一多项式集 PS, 将在有限步内计算出有限个不可约升列 IRR_k, 和关于 IRR_k 约化的非零多项式 G_k, 使得

$$\mathrm{Zero}(PS) = \bigcup_k \mathrm{Zero}(IRR_k/IP_k * G_k), \tag{3.6.130}$$

其中对每个 k, IP_k 是 IRR_k 的初式积. 等式 (3.6.130) 等价于

$$\mathrm{Zero}(PS) = \bigcup_k \mathrm{Var}[IRR_k], \tag{3.6.131}$$

$$\mathrm{Zero}(PS)=\bigcup_k \mathrm{Zero}(IRR_k/IP_k). \tag{3.6.132}$$

此外，(3.6.131) 中多余的簇可以仅通过计算消去，从而并集可变成不可缩的、且在不记顺序时唯一的形式.

证明　由 3.5 节中的零点分解定理 I 知，对于一些升列 CS_j，我们有

$$\mathrm{Zero}(PS)=\bigcup_j \mathrm{Zero}(CS_j/IP_j), \tag{3.6.133}$$

或更一般的形式：

$$\mathrm{Zero}(PS)=\bigcup_j \mathrm{Zero}(CS_j/IP_j*H_j). \tag{3.6.134}$$

在 (3.6.133) 或 (3.6.134) 中，H_j 是一些非零多项式，IP_j 是 CS_j 的初式积. 此外，每个 CS_j 的序不高于 PS 的序. 若所有 CS_j 都不可约，则无需再证. 假设存在某个 CS_j 不是不可约的. 设 $CS_j=\{C_{j1},\cdots,C_{js}\}$ 是按升序排列的，其中 C_{ji} 的类为 c_i. 假设 CS_j 为 $k-1$ 级不可约，但不是 k 级不可约的. 则 $CS_j'=\{C_{j1},\cdots,C_{j,k-1}\}$ 是不可约的，且存在类为 c_k 的多项式 F_1,F_2，类小于 c_k 的多项式 I 以及多项式 $Q_i,i=1,\cdots,k-1$，使得

$$I*C_{jk}=F_1*F_2+\sum_i^{k-1} Q_i*C_{ji}.$$

设 $CS_j^+,CS_j^{(1)},CS_j^{(2)}$ 分别为在 CS_j 中添加多项式 I,F_1,F_2 后得到的多项式集，则显然有

$$\mathrm{Zero}(CS_j)=\mathrm{Zero}(CS_j^+)+\mathrm{Zero}(CS_j^{(1)}/I)+\mathrm{Zero}(CS_j^{(2)}/I). \tag{3.6.135}$$

由定理 3.3.24 或 3.3.31 知，所有多项式集 $CS_j^+,CS_j^{(1)},CS_j^{(2)}$ 的序都低于 CS_j 的序. 对 (3.6.135) 右边的每个成员运用零点定理 I，我们可以用形如 $\mathrm{Zero}(CS'/IP'*G')$ 的零点集取代它们，其中升列 CS' 的序不高于 $CS_j^+,CS_j^{(1)}$ 或 $CS_j^{(2)}$ 的序，因而，它们的序都低于 CS_j 的序.

将 (3.6.133) 或 (3.6.134) 右边的每个成员 (其中 CS_j 不可约) 用 (3.6.130) 中的并集代替，我们仍得到一个形如 (3.6.134) 的表达式，但有不可约的 CS 的成员已被一些序更低的多项式集零点集的并代替，而这些零点集也可以按前面的方法分解. 如果新的并集中仍含有对应升列为可约的成员，则我们可以按

前面的方法用序更低的来替换. 重复使用这一方法, 根据定理 3.3.26 或 3.3.32, 这一过程将终止. 我们最后得到一个类似于 (3.6.134) 的表达式, 其中所有的升列 CS 都不可约. 把这些 CS 改写为 IRR, 则得到一个类似于 (3.6.130) 的表达式. 如果对于 (3.6.126) 右边的某个成员 G_k, 关于相应的 IRR_k 不约化, 则令 $\mathrm{Remdr}(G_k/IRR_k) = G'_k$, 从而对于 IRR_k 中多项式的初式的某一幂积 I_{G_k}, 我们有 $I_{G_k} * G_k \equiv G'_k \bmod_{\mathbf{K}} IRR_k$. 若 $G'_k = 0$, 则 $\mathrm{Zero}(IRR_k/IP_k * G_k) = \emptyset$, 且可以从 (3.6.130) 的右边去掉. 否则, 我们有 $\mathrm{Zero}(IRR_k/IP_k*G_k) = \mathrm{Zero}(IRR_k/IP_k* G'_k)$. 我们可以用 $\mathrm{Zero}(IRR_k/IP_k * G'_k)$ 来替换成员 $\mathrm{Zero}(IRR_k/IP_k * G_k)$. 因此, 我们总可以认为表达式 (3.6.130) 中所有的 G_k 都不为零且关于相应的 IRR_k 是约化的.

对于这一表达式 (3.6.130), 由定理 3.6.19 知

$$\mathrm{Zero}(PS) \subset \bigcup_k \mathrm{Var}[IRR_k]. \tag{3.6.136}$$

设 Ξ_k 为 $\mathrm{Var}[IRR_k]$ 的一个母点. 由定理 3.6.6 和 3.6.19 知, $\Xi_k \in \mathrm{Zero}(IRR_k/IP_k * G_k)$. 因此, 由 (3.6.130) 有 $\Xi_k \in \mathrm{Zero}(PS)$, 从而 $\mathrm{Var}[IRR_k] \subset \mathrm{Zero}(PS)$. 由此有

$$\bigcup_k \mathrm{Var}[IRR_k] \subset \mathrm{Zero}(PS). \tag{3.6.137}$$

综合 (3.6.136) 和 (3.6.137), 我们得到 (3.6.131). 在上面的证明中, 可取所有的 $G_k = 1$, 从而得出 (3.6.132).

最后, 由定理 3.6.25 和 3.6.27, 我们可以通过计算来确定 (3.6.132) 右边的一个簇是否包含在另一个之中. 如果是这样, 我们可以去掉这一簇. 用这种方法, 我们得到形如 (3.6.131) 的不可缩的表达式. □

定义 3.6.30 在下文中, 我们称对应于 (3.6.131) 中的不可缩的并的定理为 *簇分解定理*. 表达式 (3.6.131) 右边的在不计排列次序时唯一的分解称作簇 $\mathrm{Zero}(PS)$ 的 *不可约分解*, 其中的每个成员 $\mathrm{Var}[IRR_k]$ 称作一个 *不可约分支*.

注释 3.6.31 与定理 3.2.45 或定理 3.2.47 中所描述的簇分解定理相比, 我们看到本节的描述更一般, 而且证明是构造性的, 而以前的证明纯粹是存在性的.

若干例子

例 3.6.32 (Desargues 定理) 设 ABC 和 $A'B'C'$ 为两个三角形. 它们的对应边相互平行. 设 AA', BB' 相交于点 O, 则 CC' 通过 O.

这是例 2.1.4 中考虑过的定理的一部分．为了研究符合定理假设的几何图形，我们取坐标如下：$O=(0,0)$ 且

$$A=(x_1,0),\quad B=(0,x_3),\quad C=(x_4,x_5),$$
$$A'=(x_2,0),\quad B'=(0,x_6),\quad C'=(x_7,x_8).$$

于是定理假设等价于 $HYP=0$, 这里 HYP 是多项式集 $HYP=\{H_1,H_2,H_3\}$, 其中

$$\left.\begin{aligned} H_1&=x_1*x_6-x_2*x_3,\\ H_2&=x_4*(x_8-x_6)-x_7*(x_5-x_3),\\ H_3&=(x_4-x_1)*x_8-x_5*(x_7-x_2). \end{aligned}\right\} \tag{3.6.138}$$

为了避免繁琐的计算，我们把 x_1,x_2,x_3 看作非零的独立参数，这样实际上我们研究的就是仿射空间 $A^5_{\mathbf{K}}(x_4,\cdots,x_8)$. 多项式集 HYP 不是升列的形式．由零点分解定理容易得到

$$\text{Zero}(HYP)=\bigcup_{i=1}^{5}\text{Zero}(AS_i\ /\ IP_i), \tag{3.6.139}$$

其中 IP_i 是如下给定的升列 AS_i 的初式积：

$$\left.\begin{aligned} AS_1:\quad & x_1*x_6-x_2*x_3,\\ & (x_1*x_3-x_1*x_5-x_3*x_4)*x_7+x_2*x_4*x_5+(x_4-x_1)*x_4*x_6,\\ & (x_4-x_1)*x_8-(x_7-x_2)*x_5,\\ AS_2:\quad & x_1*x_5+x_3*x_4-x_1*x_3,\ x_1*x_6-x_2*x_3,\\ & (x_4-x_1)*x_8-x_5*(x_7-x_2),\\ AS_3:\quad & x_4,\ x_5-x_3,\ x_1*x_6-x_2*x_3,\ x_1*x_8+x_3*(x_7-x_2),\\ AS_4:\quad & x_4-x_1,\ x_5,\ x_1*x_6-x_2*x_3,\ x_1*x_8+x_3*(x_7-x_2),\\ AS_5:\quad & x_4-x_1,\ x_1*x_6-x_2*x_3,\ x_7-x_2,\ x_1*x_8-x_2*x_5. \end{aligned}\right\} \tag{3.6.140}$$

可以证明以上升列 AS_i 是不可约的，从而 (3.6.139) 可以加强为

$$\text{Zero}(HYP)=\bigcup_{i=1}^{5}\text{Var}[AS_i]. \tag{3.6.141}$$

每一簇 $\text{Var}[AS_i]$ 有一个母点 $\Xi^{(i)}$,

$$\left.\begin{aligned}
\Xi^{(1)} &= \left(x_4,\ x_5,\ \frac{x_2 * x_3}{x_1},\ \frac{x_2 * x_4}{x_1},\ \frac{x_2 * x_5}{x_1}\right),\\
\Xi^{(2)} &= \left(x_4,\ \frac{(x_1 - x_4) * x_3}{x_1},\ \frac{x_2 * x_3}{x_1},\ x_7,\ -\frac{(x_7 - x_2) * x_3}{x_1}\right),\\
\Xi^{(3)} &= \left(0,\ x_3,\ \frac{x_2 * x_3}{x_1},\ x_7,\ -\frac{(x_7 - x_2) * x_3}{x_1}\right),\\
\Xi^{(4)} &= \left(x_1,\ 0,\ \frac{x_2 * x_3}{x_1},\ x_7,\ -\frac{x_3 * (x_7 - x_2)}{x_1}\right),\\
\Xi^{(5)} &= \left(x_1,\ x_5,\ \frac{x_2 * x_3}{x_1},\ x_2,\ \frac{x_2 * x_5}{x_1}\right).
\end{aligned}\right\} \tag{3.6.142}$$

容易看出, $\Xi^{(5)}$ 是 $\Xi^{(1)}$ 在 $\mathbf{K}$ 上的一个特定化. $\Xi^{(3)},\Xi^{(4)}$ 都是 $\Xi^{(2)}$ 在 $\mathbf{K}$ 上的特定化. 从而有

$$\mathrm{Var}[AS_5] \subset \mathrm{Var}[AS_1],\ \mathrm{Var}[AS_3] \subset \mathrm{Var}[AS_2],\ \mathrm{Var}[AS_4] \subset \mathrm{Var}[AS_2].$$

另一方面, Ξ_1,Ξ_2 在 $\mathbf{K}$ 上彼此互不为特定化. 由 (3.6.141), 我们得到如下的不可缩不可约分解:

$$\mathrm{Zero}(HYP) = \mathrm{Var}[AS_1] + \mathrm{Var}[AS_2]. \tag{3.6.143}$$

图 3.1~3.5 给出了 (3.6.139) 的各种零点集对应的几何结构的简图.

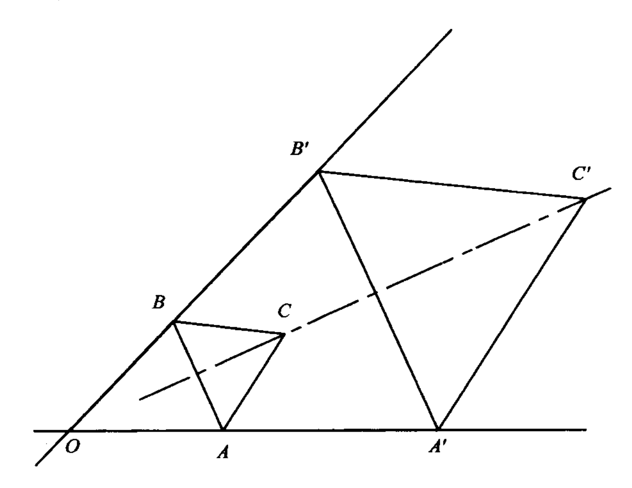


图 3.1 零点集对应的几何结构 a

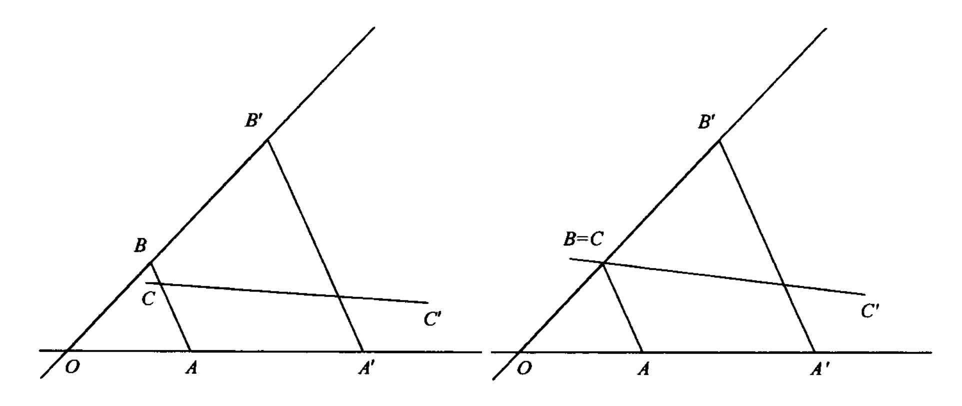


图 3.2　零点集对应的几何结构 b　　　　图 3.3　零点集对应的几何结构 c

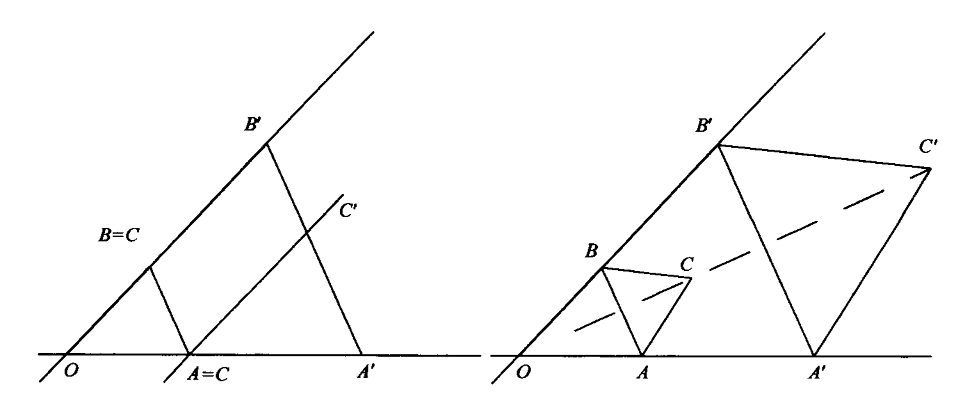


图 3.4　零点集对应的几何结构 d　　　　图 3.5　零点集对应的几何结构 e

例 3.6.33　我们考虑前面的例 3.6.32 中的不可约簇 $\mathrm{Var}[AS_1]$. 显然,

$$\mathrm{Var}[AS_1] \subset \mathrm{Zero}(AS_1).$$

设 IRR 为在 AS_1 中取如 $x_1 = 2, x_2 = 4, x_3 = 2$ 后得到的升列. 于是升列 IRR 仍是不可约的, 且 $\mathrm{Var}[IRR]$ 有一个母点

$$\Xi^{(0)} = (x_4, x_5, 4, 2 * x_4, 2 * x_5) \in \mathbf{K}^5(x_4, \cdots, x_8),$$

我们还有

$$\mathrm{Var}[IRR] \subset \mathrm{Zero}(IRR).$$

现考虑

$$X^{(0)} = (1, 1, 4, 3, 1) \in \mathbf{K}^5(x_4, \cdots, x_8).$$

容易验证， $X^{(0)} \in \mathrm{Zero}(IRR)$, 但它不是 $\Xi^{(0)}$ 在 $\mathbf{K}$ 上的一个特定化，从而不在 $\mathrm{Var}[IRR]$ 中．由此有

$$\mathrm{Var}[IRR] \subset \mathrm{Zero}(IRR) \text{ 但 } \mathrm{Var}[IRR] \neq \mathrm{Zero}(IRR).$$

同样地，我们有

$$\mathrm{Ideal}[IRR] \supset \mathrm{Ideal}(IRR) \text{ 但 } \mathrm{Ideal}[IRR] \neq \mathrm{Ideal}(IRR).$$

注释 3.6.34 不可约升列 IRR, 或更一般地， (3.6.138) 中的 AS_1 是例 3.6.32 中 Desargues 定理的假设集合 HYP 的一个特征列．也可参见 §7.3 中的例 7.3.4. $X^{(0)}$ 不在 $\mathrm{Var}[IRR]$ 或 $\mathrm{Var}[AS_1]$ 中显然具有几何意义．参见例 7.3.4 和图 3.6.

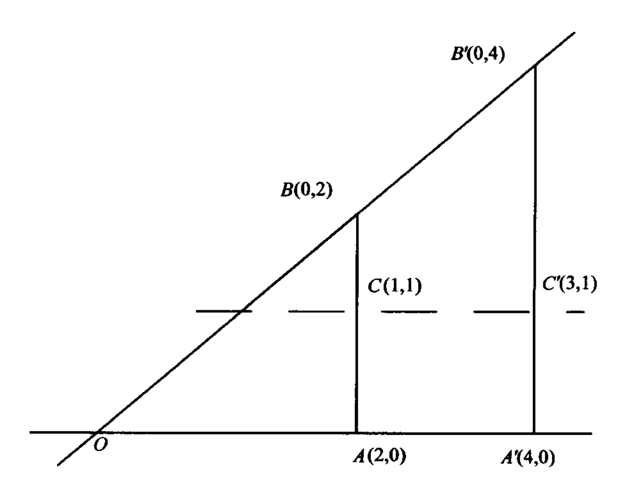


图 3.6 $X^{(0)}$ 不在 $\mathrm{Var}[IRR]$ 或 $\mathrm{Var}[AS_1]$ 中的几何意义

第四章　计算机代数的若干问题

§4.1　整数组

整数组

除非另有声明，在本章中 n 表示一个正整数.

记号 4.1.1　用 N_n 记整数集合 $\{1,2,\cdots,n\}$. 对于一个非负整数 i, 用 i^+ 记所有大于等于 i 的整数.

定义 4.1.2　一个 n- 组或者简单地一个组定义为一个有序的 n 个非负整数的序列

$$t = (I_1,\cdots,I_n),$$

t 的第 i 个坐标定义为 I_i. t 的坐标和定义为 t 的所有坐标的和.

记号 4.1.3　用 $\mathrm{Coor}_i(t)$ 记组 t 的第 i 个坐标. 用 $|t|$ 记 t 的坐标和.

定义 4.1.4　0- 组或 0- 组定义为所有坐标为零的组.

记号 4.1.5　用 0_n 或 0 记 0- 组 $(0,\cdots,0)$. 用 1_i 记组 $(\delta_{i1},\cdots,\delta_{ij},\cdots,\delta_{in})$, 其中第 j 个坐标 $=\delta_{ij}$.

定义 4.1.6　对于任意两个组 u 和 v, u 是 v 的一个倍数或 v 是 u 的一个因子，如果满足

$$\mathrm{Coor}_i(u) \geq \mathrm{Coor}_i(v), \quad i=1,\cdots,n.$$

记号 4.1.7　用 $u \gg v$ 记 u 是 v 的一个倍数，或用 $v \ll u$ 记 v 是 u 的一个因子.

定义 4.1.8　两个组 u 和 v 的乘积 $uv=vu$ 定义为满足

$$\mathrm{Coor}_i(uv) = \mathrm{Coor}_i(u) + \mathrm{Coor}_i(v), \quad i=1,\cdots,n$$

的组.

定义 4.1.9　两个组 u 和 v 的最小公倍数定义为满足

$$\mathrm{Coor}_i(l) = \max(\mathrm{Coor}_i(u),\mathrm{Coor}_i(v)), \quad i=1,\cdots,n$$

的组 l.

定义 4.1.10　两个组 u 和 v 的最大公因子定义为满足

$$\mathrm{Coor}_i(g) = \min(\mathrm{Coor}_i(u),\mathrm{Coor}_i(v)), \quad i=1,\cdots,n$$

的组 g.

记号 4.1.11 用 $\mathrm{LCM}(u,v)$ 记组 u,v 的最小公倍数. 用 $\mathrm{GCM}(u,v)$ 记组 u,v 的最大公因子.

定义 4.1.12 一个组 u 关于 u 的一个因子 v 的商 q 定义为满足

$$\mathrm{Coor}_i(q)=\mathrm{Coor}_i(u)-\mathrm{Coor}_i(v),\quad i=1,\cdots,n$$

的组 q.

记号 4.1.13 用 $\frac{u}{v}$ 记组 u 与其因子 v 的商.

<u>组的排序</u>

定义 4.1.14 对于两个组 u 和 v, 称 u 比 v 高或者 v 比 u 低, 如果存在某个 $k>0$ 和 $\leq n$, 使得

$$\begin{aligned}\mathrm{Coor}_i(u) &= \mathrm{Coor}_i(v),\quad i>k\\ \mathrm{Coor}_k(u) &> \mathrm{Coor}_k(v)\end{aligned}$$

成立.

记号 4.1.15 用 $u>v$ 记 u 比 v 高, 或用 $v<u$ 记 v 比 u 低.

定理 4.1.16 任意一个严格降序的组序列是有限的.

证明 n=1 时定理是显然的. 现在假设定理对 $(n-1)$- 组成立, 考虑 n- 组的情形. 为此让我们考虑给定的 n- 组序列的子序列, 其中的组的最后一个坐标取到最小值. 去掉最后一个坐标得到一个严格降序的 $(n-1)$- 组序列. 根据归纳假设这个 $(n-1)$- 组序列或最后一个坐标取到最小值的 n- 组构成的子序列是有限的. 因为最后一个坐标大于最小值的 n- 组个数显然有限, 给定的序列也有限. □

<u>自约化的组集合</u>

定义 4.1.17 一个组集合 T 是自约化的, 如果 T 中不存在 t 是 T 中另一个组 t' 的倍数.

定理 4.1.18 任意一个自约化的组集合 T 是有限的.

证明 n=1 时自约化集合只有一个 1- 组, 所以定理显然成立. 现在假设定理对 $(n-1)$- 组成立, 让我们考虑 n- 组的情形. 为此令 t 是给定的自约化的集合中任意一个组. 令 T_{ij} 表示由给定集合中第 i 个坐标等于 j 的组构成的子集, 这里 $0\leq j\leq \mathrm{Coor}_i(t)$. 那么这个给定的集合是自约化的, 并且是不必不相交的集合 T_{ij} 的并. 集合 T_{ij} 显然是自约化的并且其元素个数有限. 令 T'_{ij} 表示去掉 T_{ij} 中每个 n- 组的第 i 个坐标后得到的 $(n-1)$- 组构成的集合. 根

据归纳假设每个 T'_{ij} 有限. 因此每个集合 T_{ij} 是有限的, 给定的自约化的集合也是有限的. □

自约化的集合的排序

让我们考虑任意两个自约化的集合 AS 和 AS', 其中的组按照升序排列:

$$\left.\begin{array}{ll}(AS): & t_1 < t_2 < \cdots < t_r, \\ (AS)': & t'_1 < t'_2 < \cdots < t'_s.\end{array}\right\} \tag{4.1.1}$$

定义 4.1.19 自约化的集合 (AS) 比自约化的集合 $(AS)'$ 高, 或 $(AS)'$ 比 (AS) 低, 如果下面两种情形之一成立: (a) 存在某一个 $k \leq r$ 且 $\leq s$, 使得当 $i < k$ 时, $t_i = t'_i$, 且 $t_k > t'_k$; (b) $r < s$ 且当 $i \leq r$ 时, $t_i = t'_i$.

记号 4.1.20 用 $(AS) > (AS)'$ 记 (AS) 比 $(AS)'$ 高, 或用 $(AS)' < (AS)$ 记 $(AS)'$ 比 (AS) 低.

定理 4.1.21 任意一个严格降序的自约化的集合序列是有限的.

证明 假定序列是

$$(S): \quad AS_1 > AS_2 > \cdots$$

并且假设它是无限的. 对于每个自约化的集合 AS_i, 按升序排列它的组. 根据定理 4.1.16, 由 AS_i 的第 1 个组构成的序列从某项开始由同一个组构成, 假设是 t_1. 从这一项开始的自约化的集合的无穷序列记为

$$(S_1): \quad AS_{11} > AS_{12} > \cdots$$

再根据定理 4.1.16, AS_{1i} 的第 2 个组构成的序列从某项开始由同一个组构成, 假设是 t_2. 从某项开始的自约化的集合的无穷序列记为

$$(S_2): \quad AS_{21} > AS_{22} > \cdots$$

重复上面的推理, 我们得到一个无限的组序列

$$(T): \quad t_1 < t_2 < \cdots$$

这显然是一个自约化的集合. 这与定理 4.1.18 相矛盾. □

根据序的定义, 我们还得到如下的定理.

定理 4.1.22 令 AS 表示一个自约化的集合, u 是一个组, 并且不是 AS 中任意一个组的倍数. 令 AS' 表示添加 u 到 AS 中并且去掉 AS 中所有是 u 的倍数的组而得到的自约化的集合. 那么 AS' 是一个比 AS 低的自约化的集合.

证明 假定 AS 中的组是按照升序排列的, 形如 (4.1.1), 那么 $t_k < u < t_{k+1}$, 对于某个 $0 < k < r$, 或者 $u < t_1$ 或者 $t_r < u$. 无论哪种情况, 通过添加到 AS 中并且去掉 AS 中所有 u 的倍数而得到的组集合是一个比 AS 低的自约化的集合. □

完备化和完备的组集合

定义 4.1.23 对于任意一个有限的组集合 T,T 的极大组定义为组

$$\max(T) = (\max_1(T), \cdots, \max_n(T)),$$

这里

$$\max_i(T) \ = \ \max\{\mathrm{Coor}_i(t) \mid t \in T\}.$$

定义 4.1.24 对于任意一个有限的组集合 T, T 的完备化定义为组集合

$$\left\{u \mid u \ll \max(T), \text{且存在 } T \text{ 中的某一个 } t, \text{使得 } u \gg t\right\}.$$

记号 4.1.25 用 $\mathrm{Comp}(T)$ 记组集合 T 的完备化.

定义 4.1.26 一个有限的组集合 CT 是完备的, 如果 CT 是其自身的完备化, 或 $CT = \mathrm{Comp}(CT)$.

定理 4.1.27 对于任意一个完备的组集合 CT, 存在唯一的自约化的组集合 $T \subset CT$, 使得 $CT = \mathrm{Comp}(T)$. 此外, 有一个算法在有限步内从 CT 得到 T.

证明 让我们把 CT 中的组按照降序 $t_1 > t_2 > \cdots > t_N$ 排列. 从第一步 $i = 1$ 开始到 $i = N$, 让我们去掉 t_i, 如果它是 CT 中某一个比 t_i 低的组的倍数, 那么最后剩下的组集合 T 显然是一个所要求的自约化的集合. 这样的自约化的组集合的唯一性可在下面的论述中看到.

假设 T',T'' 是两个包含在 CT 中的自约化的组集合, 使得 $CT=\mathrm{Comp}(T') = \mathrm{Comp}(T'')$. 让我们分别按降序: $t'_1 > \cdots > t'_{n'}$, $t''_1 > \cdots > t''_{n''}$ 重排 T' 和 T'' 中的组. 假设 $t''_1 \neq t'_1$. t'_1, 因为在 CT 中, 应当是 T'' 中某个组比如 t''_i 的倍数. 类似地 t''_i 应当是 T' 中的某个组比如 t'_j 的一个倍数. 那么 t'_1 是 t'_j 的一个倍数. 由于 T' 是自约化的, 我们必有 $t'_1 = t'_j$, 进而又有 $t'_1 = t''_i$. 因为 $t''_1 \neq t'_1$, 有 $t''_1 \neq t''_i$, 这样 $t''_1 > t''_i$ 或者 $t''_1 > t'_1$. 同样, 如果 $t'_1 \neq t''_1$, 则 $t'_1 > t''_1$. 这就导出矛盾, 因此必须有 $t'_1 = t''_1$. 同样的推理表明 $t'_2 = t''_2$, 等等. $n' = n''$ 是显然的, 正如要证明的那样 $T' = T''$. □

定义 4.1.28 一个完备的组集合 CT 的收缩定义为唯一的自约化的组集合 $T \subset CT$, 其使得 $\mathrm{Comp}(T) = CT$.

记号 4.1.29　用 Cont(CT) 记完备的组集合 CT 的收缩.

下面的两个定理可以直接由定义得到.

定理 4.1.30　对于一个自约化的组集合 T, 我们有

$$\text{Cont Comp}(T) = T.$$

定理 4.1.31　对于一个完备的组集合，我们有

$$\text{Comp Cont}(CT) = CT.$$

<u>乘子和非乘子</u>

定义 4.1.32　对于任意一个有限的组集合 T 和任意一个组 $t \ll \max(T)$, 整数 i $(1 \le i \le n)$ 是 t 关于 T 的一个乘子，如果

$$\text{Coor}_i(t) \;=\; \max_i(T).$$

相反地，i 是 t 关于 T 的一个非乘子，如果

$$\text{Coor}_i(t) \;<\; \max_i(T).$$

记号 4.1.33　对于任意的一个有限的组集合 T 和任意的一个组 $t \ll \max(T)$, 用 Mult(t/T) 记 t 关于 T 的所有乘子的集合，用 Nult(t/T) 记 t 关于 T 的所有非乘子的集合.

<u>组分解定理</u>

定义 4.1.34　一个有限的组集合 T 的全部倍数集定义为 T 中某个组的所有倍数的集合.

定义 4.1.35　对于 $t \ll \max(T)$, t 的关于 T 的全部倍数集定义为 t 的所有倍数 tv 构成的集合，这里

$$\text{Coor}_i(v) = 0, \quad i \in \text{Nult}(t/T).$$

记号 4.1.36　用 TMS(T) 记组集合 T 的全部倍数集. 用 TMS(t/T) 记 t 的关于组集合 T 的全部倍数集.

定理 4.1.37　T 是一个有限的组集合. 对于任意一个组 $u \in \text{TMS}(T)$, 存在唯一的组 $t \in \text{Comp}(T)$, 使得对于某个组 v, 有 $u = tv$,

$$u\text{在TMS}(t/T)\text{中}$$

或

$$\text{Coor}_i(v) = 0, \quad i \in \text{Nult}(t/T).$$

此外，如果 u 本身在 T 中，那么 $t = u$.

证明 t 通过 $\text{Coor}_i(t) = \min(\text{Coor}_i(u), \max_i(T))$ 确定. □

定义 4.1.38 对于一个有限的组集合 T, 一个组 $u \in \text{TMS}(T)$ 的核定义为定理 4.1.37 中确定的唯一的组 $t \in \text{Comp}(T)$. 对应地, u 定义为 $t \in \text{Comp}(T)$ 的一个覆盖.

记号 4.1.39 用 $\text{Ker}(u/T)$ 记 u 的关于 T 的核.

定理 4.1.40 (组分解定理) 对于任意一个有限的组集合 T, T 的全部倍数集是集合 $\text{TMS}(t/T)$ 的不交并集, t 取遍 $\text{Comp}(T)$.

证明 对于任意一个组 $u \in \text{TMS}(T)$, 我们有 $u \in \text{TMS}(t/T)$, 这里 $t = \text{Ker}(u/T) \in \text{Comp}(T)$. 因此

$$\text{TMS}(T) = \bigcup_{t \in \text{Comp}(T)} \text{TMS}(t/T),$$

其中并对所有的 $t \in \text{Comp}(T)$ 取. 显然这些 $\text{TMS}(t/T)$ 彼此不相交. □

t 关于 T 的全部倍数集可以在下面易证的定理中进一步细化.

定理 4.1.41 对于一个组 $t = (i_1, \cdots, i_j, \cdots, i_n) \in \text{Comp}(T)$, 我们有

$$\text{TMS}(t/T) = \{(i'_1, \cdots, i'_j, \cdots, i'_n) \mid (*)\}, \tag{4.1.2}$$

其中 $(*)$ 是指

$$\left.\begin{aligned} i'_j &= i_j, \quad \text{如果 } i_j \in \text{Nult}(t/T), \\ i'_j &\in i_j^+, \quad \text{如果 } i_j \in \text{Mult}(t/T). \end{aligned}\right\} \tag{4.1.3}$$

<u>一个例子</u>

例 4.1.42 考虑一个组集合 $T = \{t_1, t_2, t_3\}$, 其中

$$t_1 = (0,0,2), \qquad t_2 = (0,1,1), \qquad t_3 = (1,0,1),$$

则我们有 $t_1 > t_2 > t_3, \max(T) = (1,1,2)$ 及

$$\begin{aligned} \text{Comp}(T) &= \{1_1 1_2 t_1,\ 1_2 t_1,\ 1_1 t_1,\ t_1,\ 1_1 t_2,\ t_2,\ t_3\} \\ &= \{(1,1,2),\ (0,1,2),\ (1,0,2),\ (0,0,2),\ (1,1,1),\ (0,1,1),\ (1,0,1)\}. \end{aligned}$$

上述的这些组的乘子集 (按上述次序) 分别是

$$\{1,2,3\},\ \{2,3\},\ \{1,3\},\ \{3\},\ \{1,2\},\ \{2\},\ \{1\}.$$

相应的非乘子集分别是

$$\emptyset,\ \{1\},\ \{2\},\ \{1,2\},\ \{3\},\ \{1,3\},\ \{2,3\}.$$

t 关于 T 的全部倍数集如下：

$$\begin{aligned}
\mathrm{TMS}(1,1,2) &= \{(1^+,1^+,2^+)\},\\
\mathrm{TMS}(0,1,2) &= \{(0,1^+,2^+)\},\\
\mathrm{TMS}(1,0,2) &= \{(1^+,0,2^+)\},\\
\mathrm{TMS}(0,0,2) &= \{(0,0,2^+)\},\\
\mathrm{TMS}(1,1,1) &= \{(1^+,1^+,1)\},\\
\mathrm{TMS}(0,1,1) &= \{(0,1^+,1)\},\\
\mathrm{TMS}(1,0,1) &= \{(1^+,0,1)\}.
\end{aligned}$$

组集合的其他几种排序

注释 4.1.43 本节所给出的组的排序，是所谓的 *逆字典序*. 有时其他的排序比 *逆字典序* 更方便. *坐标和序*(coor-sum ordering), 就是这样的一种排序；一个组 u 比组 v 高，如果 $|u|>|v|$ 或者 $|u|=|v|$ 同时在 *逆字典序* 中 $u>v$. 进一步的概念和结果可以像前面那样平行地建立，并且没有本质的差异. 除非另有声明，我们仍采用 *逆字典序*.

§4.2 多项式理想的良序基

环 $\mathbf{K}[x_1,\cdots,x_n]$ 中的多项式

除非另有说明，本章中将假定 n 为整数，$X=(x_1,\cdots,x_n)$ 为一个变量集合，$\mathbf{K}$ 为一个特征为零的域.

定义 4.2.1 一个单项式定义为形如下面的关于 x_i 的一个幂积：

$$X^t = x_1^{i_1}*\cdots*x_j^{i_j}\cdots*x_n^{i_n},\quad 其中t=(i_1,\cdots,i_n).$$

显然对于任意两个组 u,v, 我们有

$$X^u*X^v = X^{uv}.$$

定义 4.2.2 单项式 X^t 的次数组 (degree-tuple) 定义为 t.

定义 4.2.3 一个非零多项式 P 具有正规形式，如果

$$P = a_1*X^{t_1}+a_2*X^{t_2}+\cdots+a_r*X^{t_r}, \tag{4.2.4}$$

其中 a_i 为 $\mathbf{K}$ 中非零元素，且次数组 t_i 按降序排列，即

$$t_1 > t_2 > \cdots > t_r. \tag{4.2.5}$$

对于 P, 这样的正规形式显然是唯一的.

定义 4.2.4 对于如上正规形式的多项式 P,

$a_1 * X^{t_1}$ 称作 P 的首项 (leading term),

X^{t_1} 称作 P 的首单项式 (leading monom),

a_1 称作 P 的首项系数 (leading coefficient),

t_1 称作 P 的首次数组 (leading degree-tuple).

记号 4.2.5 用 Lterm(P) 记 P 的首项,

用 Lmonom(P) 记 P 的首单项式,

用 Lcoef(P) 记 P 的首项系数,

用 Ldeg(P) 记 P 的首次数组.

<u>多项式的一种偏序</u>

定义 4.2.6 对于两个非零多项式 P_1 和 P_2, P_1 高于 (或低于, 不可比于) P_2 是指 P_1 的首次数组 高于 (或低于, 不可比于) P_2 的首次数组.

记号 4.2.7 对于两个非零多项式 P_1, P_2,

用 $P_1 > P_2$ 记 P_1 高于 P_2;

用 $P_1 < P_2$ 记 P_1 低于 P_2;

用 $P_1 <> P_2$ 记 P_1, P_2 是不可比的.

<u>自约化的多项式集合</u>

通过一个多项式集合中多项式的次数组, 我们像下面那样把有关次数组的概念移植到多项式集合上.

定义 4.2.8 对于一个多项式集合 PS, PS 的次数组集合定义为 PS 中多项式的首次数组构成的集合.

记号 4.2.9 用 DTS(PS) 记 PS 的次数组集合.

定义 4.2.10 一个多项式集合 PS 是 自约化 (autoreduced) 的, 如果 PS 的次数组集合是自约化的.

定义 4.2.11 令 AS 是一个自约化的多项式集合, $T = \mathrm{DTS}(AS)$ 是它的次数组集合. 一个非零多项式 P 关于 AS 是约化的, 如果对于 P 中的每一项, 相应的次数组不是 T 中任何一个组的倍数.

定义 4.2.12 一个自约化的多项式集合 AS 是约化的, 如果 AS 的每个多项式关于从 AS 中去掉这一多项式后得到的自约化的多项式集合是约化的.

<u>自约化的多项式集合的偏序</u>

定义 4.2.13 对于两个自约化的多项式集合 AS_1 和 AS_2, AS_1高于, 低于, 或不可比于 AS_2, 如果 AS_1 的次数组集合分别 高于, 低于, 或恒等于 AS_2

的次数组集合.

记号 4.2.14　对于两个自约化的多项式集合 AS_1, AS_2,

用 $AS_1 > AS_2$ 记 AS_1 高于 AS_2;

用 $AS_1 < AS_2$ 记 AS_1 低于 AS_2;

用 $AS_1 <> AS_2$ 记 AS_1, AS_2 关于序是不可比的.

定理 4.2.15　一个给定多项式集中的任意两个具有最低序的自约化的多项式集合关于序是不可比的.

证明　这可直接由定义推出. □

<u>多项式集合的偏序</u>

定理 4.2.15 允许我们在下面定义中对于任意的多项式集合引入偏序关系.

定义 4.2.16　对于两个多项式集合 PS_1 和 PS_2, PS_1高于, 低于, 或不可比于 PS_2, 如果对于 PS_1 中任意一个最低序次的自约化的多项式子集 高于, 低于, 或不可比于 PS_2 中任意一个最低序次的自约化的多项式子集.

记号 4.2.17　用 $PS_1 > PS_2$ 记 PS_1 高于 PS_2;

用 $PS_1 < PS_2$ 记 PS_1 低于 PS_2;

用 $PS_1 <> PS_2$ 记 PS_1, PS_2 关于序是不可比的.

定理 4.2.18　给定一个多项式集合 PS, 令 R 是一个关于 PS 中任意一个具有最低序次的自约化子集是约化的多项式, 那么把多项式 R 添加到 PS 中得到的多项式集比原来的多项式集 PS 低.

证明　这可由定义和定理 4.1.22 得出. □

注释 4.2.19　上面定理给出了降低多项式序次的一个方法.

<u>关于一个自约化的多项式集合的约化式 (rests)</u>

对于一个由非零多项式 A_i 组成的自约化的多项式集合 AS, 可以有多种方法把一个多项式 P 写成如下形式:

$$P = \sum_i E_i * A_i + R$$

或 (4.2.6)

$$P \equiv R \bmod_{\mathbf{K}} AS,$$

其中 E_i, R 为多项式, 且 R 如果非零, 则关于 AS 是约化的. 可参看下面的例子:

例 4.2.20　令 $AS = \{A_1, A_2\}$ 是一个自约化的集合,

$$A_1 = x_1 * x_2 - 1,\ A_2 = x_2^2 - 1,$$

那么多项式

$$P = x_1 * x_2^2 + x_2^2 + x_1^2 * x_2$$

可以写成下面两种形式:

$$P \;=\; x_1 * A_1 + (x_1 + 1) * A_2 \;+ (2 * x_1 + 1)$$

或

$$P \;=\; (x_1 + x_2) * A_1 + A_2 + (x_1 + x_2 + 1),$$

因此 R 可以是 $2 * x_1 + 1$ 或者 $x_1 + x_2 + 1$, 不是唯一的.

为了从 P 得到一个唯一的 R, 让我们按如下步骤进行. 令 T 是 AS 的次数组集合. 把 P 写成正规形式. 令 $c * X^t$ 是 P 的非零项, 其中 c 在 $\mathbf{K}$ 中, 使得 t 是 T 中某一个组的倍数并且最高的序次, 如果存在的话. 一旦取定 t, 则 u 取作 T 中具有最高序次的组使得 t 是它的倍数. 现在记作 $t = uv$. 假设 AS 中以 u 为首次数组的多项式具有如下形式:

$$A_i \;=\; a * X^u + A_i',$$

其中 $a * X^u$ 为 A_i 的首项, $a \neq 0$ 在 $\mathbf{K}$ 中. 令

$$P_1 \;=\; P \;-\; \frac{c}{a} * X^v * A_i,$$

那么 P_1 是这样的一个多项式, P_1 中最高序次的项其次数组 t_1 是 T 中某一个组的倍数, 如果存在的话, 它比上面的 t 具有较低的序次. 然后我们可以对 P_1 用与前面同样的步骤得到一个多项式 P_2. 根据定理 4.1.16, 这个过程必在有限步内终止. 最后得到一个多项式 P_s, 它关于 AS 是约化的. 这个 P_s 就是所需要的 R.

定义 4.2.21 一个多项式 P 关于自约化的多项式集合 AS 的约化式定义为以上面的方式由 P 而得到的唯一的关于 AS 是约化的多项式 R.

P 关于 AS 的子约化式 (subrest) 定义为满足 (4.2.6) 式的、关于 AS 是约化的任意一个非零多项式 R.

记号 4.2.22 用 $\mathrm{Rest}(P/AS)$ 记 P 关于自约化的多项式集合 AS 的约化式 rest.

例 4.2.23 对于例 4.2.20 中的 AS 和 P, 我们有 $\mathrm{Rest}(P/AS) = 2 * x_1 + 1$. $x_1 + x_2 + 1$.$2 * x_1 + 1$ 和 $x_1 + x_2 + 1$ 都是 P 关于 AS 的子约化式.

我们把上面所述以定理的形式总结如下:

定理 4.2.24 给定一个自约化的多项式集合 AS, 对于每个 P 存在唯一的一个关于 AS 是约化的多项式 R, 使得

$$P \equiv R \bmod_{\mathbf{K}} AS,$$

其中 (4.2.7)

$$R = \mathrm{Rest}(P/AS).$$

定义 4.2.25 (4.2.7) 式及由 (4.2.7) 式给出的 R 称作 P 关于自约化的多项式集合 AS 的约化公式.

注释 4.2.26 根据定理 4.2.18 和注释 4.2.19, 我们看到为了降低一个多项式集合的序次, 只需通过添加那个多项式集合的具有最低序次的某一个自约化的多项式集合的非零约化式来扩大多项式集合就可以了. 这就导出了多项式集的良序基 (well-arranged basis) 的概念. 它的构造下面给出.

一个自约化的多项式集合的约化

定理 4.2.27 存在一个算法, 可以把任意一个给定的自约化的多项式集合 AS 化为约化的自约化的多项式集合 AS', 并且有其相同的次数组集合.

证明 让我们按降序 $A_1 > A_2 > \cdots > A_N$ 排列 AS 中的多项式. 令 $A'_N = A_N$ 及 $AS'_N = \{A'_N\}$. 从 $i = N-1, N-2, \cdots, 1$, 我们可以逐步地得到 A_i 关于自约化的多项式集合 $AS'_{i+1} = \{A'_{i+1}, \cdots, A'_N\}$ 的约化式 A'_i. 那么最后得到的多项式集合 AS'_1 就是要求的自约化的多项式集合 AS'. □

定义 4.2.28 一个自约化的多项式集合 AS 的约化定义为在定理 4.2.27 的证明中所描述的过程.

一个多项式理想的良序基

记号 4.2.29 以多项式集 PS 作为基的多项式理想记作 $\mathrm{Ideal}(PS)$.

定义 4.2.30 一个以 PS 为基的多项式理想 $\mathrm{Ideal}(PS)$ 的良序基 (well-arranged basis) 定义为作为理想的一个基的一个自约化的多项式集合 WAS, 使得 $\mathrm{Ideal}(WAS) = \mathrm{Ideal}(PS)$.

给定一个任意的有限的非零多项式集合 PS, 让我们构造如下的方案 (A):

$$\begin{array}{lllll} PS = & PS_0 & PS_1 & \cdots & PS_r \\ & AS_0 & AS_1 & \cdots & AS_r \\ & RS_0 & RS_1 & \cdots & RS_r = \emptyset \end{array} \tag{A}$$

上述方案按如下步骤进行:

对于任意一个 i, AS_i 是一个具有最低序次的自约化的多项式集合, 其中多项式取自 PS_i, 使得 PS_i 中任一剩余的多项式的次数组是 AS_i 中某一个多项式的次

数组的倍数. 每一个 RS_i 是 $PS_i \setminus AS_i$ 中多项式关于 AS_i 所作的非零约化式的集合 (如果存在的话). 多项式集 PS_{i+1} 是之前的 AS_i 和 RS_i 的并集:

$$PS_{i+1} = AS_i + RS_i. \tag{4.2.8}$$

从上面的构造步骤看到, 根据定理 4.2.18, 自约化集 AS_i 是严格降序的:

$$AS_0 > AS_1 > \cdots,$$

所以 AS_i 的次数组集合是严格降序的. 根据定理 4.1.21, 这个序列是有限的, 所以上面步骤在有限步内终止. 相应的非零约化式集 $RS_r = \emptyset$. 如图表 (A) 所示.

定理 4.2.31 方案 (A) 中最终得到的自约化的集合 AS_r 构成以 PS 作为基的理想 $\mathrm{Ideal}(PS)$ 的一个良序基, 而且 $\mathrm{Ideal}(PS) = \mathrm{Ideal}(AS_r)$.

证明 令 AS_0 由多项式 P_i 和 PS_0 的中多项式 Q_j 组成, 使得 $\mathrm{Ideal}(PS)$ 有一个基由 P_i 和 Q_j 组成. 令 $R_j = \mathrm{Rest}(Q_j/AS_0)$. 那么, 由 Q_j 关于 AS 的约化公式, 显然有 $\mathrm{Ideal}(PS_0) = \mathrm{Ideal}(PS_1)$. 继续下去, 我们有

$$\mathrm{Ideal}(PS) = \mathrm{Ideal}(PS_0) = \mathrm{Ideal}(PS_1) = \cdots = \mathrm{Ideal}(PS_r).$$

由于对于任意 $P \in PS_r$, $\mathrm{Rest}(P/AS_r) = 0$, 我们也有 $\mathrm{Ideal}(PS_r) = \mathrm{Ideal}(AS_r)$, 所以 $\mathrm{Ideal}(PS) = \mathrm{Ideal}(AS_r)$. AS_r 就是要求的良序基. □

例 4.2.32 重新考虑 Czapor 和 Geddes 的例 3.4.21 和 3.5.32. 对于多项式集合 $PS = P_1, P_2, P_3$, 其中 P_i 由 (3.4.48) 给出, 并让我们再次取定序次: $x \prec y \prec z$, 那么自约化的集合 $WAS_0 = \{W_1, W_2, W_3\}$,

$$W_1 = P_3,\ W_2 = P_1,\ W_3 = P_2, \tag{4.2.9}$$

是按降序排列的自约化的集合. 这已经是理想 $\mathrm{Ideal}(PS)$ 的一组良序基. WAS_0 的首次数组集合为 $T = \{t_1, t_2, t_3\}$, 其中

$$t_1 = (0,0,2) > t_2 = (0,1,1) > t_3 = (1,0,1),$$

如同在例子 4.1.42 中所讨论的一样.

一个多项式理想的 Gröbner 基

在当前的文献中多项式的 Gröbner 基 是一个广泛应用的概念. 我们在这里仅给出其定义和与本书主要目的密切相关的性质.

定义 4.2.33 对一个多项式理想 $ID \subset \mathbf{K}[X]$, 一个自约化的多项式集合 GB 是 ID 的一个 Gröbner 基, 如果 GB 是 ID 的一个基, 且 ID 中任意一个多项式 P 关于 GB 的 (所有) 子约化式都等于零.

定义 4.2.34　对于一个多项式理想 $ID \subset \mathbf{K}[X]$, 一个自约化的多项式集合 GB 是 ID 的一个约化的 Gröbner 基, 如果 GB 是 ID 的一个 Gröbner 基, 且作为一个自约化的集合是约化的.

定理 4.2.35 (Buchberger)　对于一个多项式集合 $PS \subset \mathbf{K}[X]$. 设 GB 为 $\mathrm{Ideal}(PS)$ 的一个 Gröbner 基. 那么 $\mathrm{Zero}(PS) = \emptyset$ 当且仅当存在某个非零常数 $k \in \mathbf{K}$, 使得 $k \in GB$. 进一步, $\mathrm{Zero}(PS)$ 是非空有限的当且仅当它是非空的, 且对任意一个 $i, 1 \leq i \leq n$, 存在一个 GB 中的多项式, 其首单项式为某一个 x_i 的幂次.

证明　参见 Buchberger 的原始文献 [Bu1].

注释 4.2.36　一个理想的 (约化的)Gröbner 基有许多很好的性质, 在本书中不会涉及. 不过在后面几节中将引入多项式理想的某种基, 证明其在本质上等价于约化的 Gröbner 基并且有同样好的性质. 但我们是以一种与当前 Gröbner 基研究方式完全不同的方式引入的.

§4.3　一个多项式理想的良性基

基于 Riquier-Janet 理论的一个基的构造原理

对于给定的以 PS 为基底的一个多项式理想 (或一个代数簇), 其 Gröbner 基 GB 要求这个给定的理想中的所有多项式关于 GB 的约化式为 0. 由于理想中的多项式个数是无限的, 后一个要求初看之下难以实现. Buchberger 准则表明可把此要求限制在某一个有限的多项式集合 S 多项式, Buchberger 算法正是基于此准则. 另一方面, 作者在研究 Riquier 及 Janet 关于偏微分方程的理论时, 发现了构造 Gröbner 基的另一种方法. 参见 [Rig], [Jan]. 当偏微分方程组是线性的, 系数为常数, 且关于一个未定元的系数为常数时, 此方程与一普通多项式方程相对应, 我们实际在讨论普通多项式理想. Riquier-Janet 算法给我们这个理想某一个基, 其具有良好的性质. 为此我们称如此得到的基为多项式理想的良性基. 这表明此良性基的一个子基即是此给定理想的一个 Gröbner 基. 这种替代的方法的本质在于, 其没有像在构造良序基的方案 (A) 中, 求多项式的约化式; 其也没有如构造 Gröbner 的方案 (B) 中求 S 多项式的约化式. 而是按特定的方式计算单变量多项式乘积的约化式. 下面我们将详述此方法, 对此可参见原始文献 [WWT18].

自约化的多项式集合的完备化

除非另有声明, 下面的 AS 将表示一个自约化的多项式集合, 其次数组集

合为 T.

记号 4.3.1 对于任意一个 $t\in T$, 用 A_t 记 AS 中以 t 为其次数组的多项式.

定义 4.3.2 对于任意一个 $u\in \mathrm{Comp}(T), AS$ 相对于 u 的完备的多项式定义为多项式 $X^v * A_t$, 其中 $u=tv$, t 是 T 中以 u 为倍数的最高序次的组.

记号 4.3.3 对于 $u\in \mathrm{Comp}(T)$, 用 H_u 记 AS 相对于 u 的完备的多项式.

定义 4.3.4 AS 的完备化定义为所有 AS 中的相对于 $u\in \mathrm{Comp}(T)$ 是完备的多项式 H_u 构成的多项式集合.

定义 4.3.5 完备的多项式集合定义为某一个自约化的多项式集合的完备化.

定义 4.3.6 一个完备的多项式集合的收缩定义为一个自约化的多项式集合，这个完备的多项式集合为它的完备化.

记号 4.3.7 用 $\mathrm{Comp}(AS)$ 记 AS 的完备化，其中 AS 为一个自约化的多项式集合.

记号 4.3.8 用 $\mathrm{Cont}(CPS)$ 记 CPS 的收缩，其中 CPS 是一个完备的多项式集合.

由定义，下述两定理是显然的.

定理 4.3.9 对于任意一个自约化的多项式集合 AS,

$$\mathrm{ContComp}(AS)=AS. \tag{4.3.10}$$

定理 4.3.10 对于任意一个完备的多项式集合 CPS,

$$\mathrm{CompCont}(CPS)=CPS. \tag{4.3.11}$$

<u>关于一个完备的多项式集合的 M- 积和 M- 多项式</u>

除非另有声明，以下 CPS 是以 CT 为其次数组集合的完备的多项式集合，H_u 是其完备的多项式，$u\in CT, AS$ 是其收缩.

定义 4.3.11 CPS 的一个 M- 积定义为具有 $X^v * H_u$ 形式的乘积，其中 H_u 是 CPS 中以 $u\in CT$ 为其次数组的多项式，而且 i 使 $\mathrm{Coor}_i(v)\neq 0$ 的 i 是 u 的一个乘子，或 uv 是如定义 4.1.38 所示的 u 的一个覆盖.

定义 4.3.12 CPS 的一个 M- 多项式定义为 CPS 中在 $\mathbf{K}$ 上 M- 积的有限的线性组合.

<u>多项式关于一个完备的多项式集合的标准表示</u>

定理 4.3.13 任意一个多项式 P 可唯一地表示成下述形式:

$$\left.\begin{array}{rl} P = & M+N, \\ M = & \sum\limits_{u,v} C_{uv} * X^v * H_u. \end{array}\right\} \tag{4.3.12}$$

在 (4.3.12) 中 M 是一个 M- 多项式， $c_{uv} \in \mathbf{K}$ 不等于 0, $X^v * H_u$ 是互不相同的 M- 积，此外 N 关于 $AS = \mathrm{Cont}(CPS)$ 是约化的.

证明　假设 P 关于 AS 不是约化的. 那么 P 中关于 AS 非约化的项中，有一个最高序次的项 $a * X^w$, 其中 $a \neq 0$. 由 (4.1) 中组分解定理知，有唯一的一个 $u \in CT$, 使得 $w = uv$ 是 u 的一个覆盖. 令 H_u 是 CPS 中以 u 为首次数组的完备的多项式，其首项 $\mathrm{Lterm}(H_u) = b * X^u$. 取

$$P_1 = P/a - X^v * H_u/b,$$

即

$$P = c_1 * M_1 + b_1 * P_1 \quad (c_1 = a/b, b_1 = a),$$

其中 $M_1 = X^v * H_u$ 是一个 M- 积. 如果 P_1 关于 AS 不是约化的，那么在 P_1 中关于 AS 非约化的项中，有一个最高项 $a_1 * X^{w_1}$, 其中 a_1 属于 $\mathbf{K}$ 不等于 0. 应用上述步骤于 P_1, 我们可得多项式 P_2, 使得 $P_1 = c_2 * M_2 + b_2 * P_2$, 其中 b_2, c_2 属于 $\mathbf{K}$, 而 M_2 是一个 M- 积，其序次低于 M_1. 上述方法可继续得到 P_3 等等. 根据关于首次数组的定理 4.1.16, 可知我们能在有限步内得一关于 AS 是约化的多项式 P_r. 那么我们可把 P 表达成 (4.3.12) 的形式，其中 M 是一 M-多项式， $N = b_r * P_r$ 关于 AS 是约化的，如所要求的那样. 此分解的唯一性易由组分解定理 4.1.40 得到. □

定义 4.3.14　(4.3.12) 称为 P 关于完备的多项式集合 CPS 的标准表示.

定义 4.3.15　(4.3.12) 中的多项式 M 和 N 分别称为 P 关于完备的多项式集合 CPS 的 M- 部分和 N- 部分.

<u>一个完备的多项式集合的 N- 多项式和 N- 多项式集合</u>

考虑 CT 中的任意一个 u, H_u 是相应的完备的多项式, i 是 u 的任意一个非零乘子. 那么 $1_i u = w$ 也在 CT 中，可把 $x_i * H_u$ 分解成下述 M- 部分及 N-部分：

$$x_i * H_u = a * H_w + M_{iu} + N_{iu}, \tag{4.3.13}$$

其中 a 在 $\mathbf{K}$ 中不等于 $0, M_{iu}$ 是一个 M- 多项式，其每一个 M- 积序次均低于 H_w 或 $x_i * H_u$, N_{iu} 是 $x_i * H_u$ 的 N- 部分. 注意 N_{iu} 关于 $AS = \mathrm{Cont}(CPS)$ 是约化的，由于其重要性，我们给出下述定义：

定义 4.3.16 (4.3.13) 中多项式 $x_i * H_u$ 的 N- 部分 N_{iu} 称为完备的多项式集合 CPS 关于组 $u \in CT$ 及非乘子 $i \in \mathrm{Nult}(u/CT)$ 的 N- 多项式.

构造一个多项式理想基的方案 (W)

现在考虑一个有限的多项式集合 PS, 我们构造下述方案 (W):

$$\begin{array}{lllll} PS = & PS_0 & PS_1 & \cdots & PS_s \\ & WAS_0 & WAS_1 & \cdots & WAS_s \\ & NS_0 & NS_1 & \cdots & NS_s & = \emptyset \end{array} \tag{W}$$

此方案可由下述步骤构造:

对于每一个 i, WAS_i 是理想 $\mathrm{Ideal}(PS_i)$ 的一个良序基, 它是把 4.2 节的方案 (A) 应用到 PS_i 所得到的. NS_i 是由 $\mathrm{Comp}(WAS_i)$ 的所有非零的 N- 多项式构成的集合, 如果存在的话. 最终, PS_{i+1} 是下述集合的并:

$$PS_{i+1} = WAS_i + NS_i. \tag{4.3.14}$$

与方案 (A) 相似, 自约化的集合序列 WAS_i 是严格降序的, 所以上述步骤将会在某一步终止, 此时 $NS_s = \emptyset$, 如上表 (W) 所示.

定理 4.3.17 在方案 (W) 中最终得到的良序集 WAS_s 是理想 $\mathrm{Ideal}(PS)$ 的一个基, 或者

$$\mathrm{Ideal}(PS) = \mathrm{Ideal}(WAS_s).$$

证明 根据定理 4.2.15, 我们有 $\mathrm{Ideal}(PS_i) = \mathrm{Ideal}(WAS_i)$. NS_i 中的每个多项式 N 是某个 $x_k * H_u$ 的 N- 部分相对于 $CT_i = \mathrm{Comp}(T_i)$ 中组 u 和非乘子 k, 其中 H_u 是 $CPS_i = \mathrm{Comp}(WAS_i)$ 中相对于 $CT_i = \mathrm{Comp}(T_i)$ 中组 u 完备的多项式, T_i 是 WAS_i 的次数组集合, $k \in \mathrm{Nult}(u/CT_i)$, 并满足 $x_k * H_u = M_{ku} + N_{ku}$, 其中 M_{ku}, N_{ku} 分别是相应的 M- 部分及 N- 部分. 根据表达式可知, 对每一对 (k, u) 有 $N_{ku} \in \mathrm{Ideal}(PS_i)$, 这样我们可得

$$\mathrm{Ideal}(PS_i) = \mathrm{Ideal}(PS_i + NS_i) = \mathrm{Ideal}(WAS_i + NS_i) = \mathrm{Ideal}(PS_{i+1}),$$

最终

$$\mathrm{Ideal}(PS) = \mathrm{Ideal}(PS_0) = \mathrm{Ideal}(PS_1) = \cdots = \mathrm{Ideal}(PS_s) = \mathrm{Ideal}(WAS_s),$$

正如要被证明的那样. □

一个多项式理想的良性基

定义 4.3.18 一个多项式理想 Ideal(PS) 的一个良性基定义为一个完备的多项式集合 WB 且其是理想 Ideal(PS) 的一个基的收缩，且满足下述性质：

对于完备的多项式集合 WB 中的任意一个多项式 H_u 和任意一个 WB 的次数组集 CT 中元素 u 的非乘子 i, $x_i * H_u$ 关于 WB 的 N- 部分为 0.

定义 4.3.19 一个多项式理想的一个良性基是约化的，如果 WB 的收缩是一个约化的自约化的多项式集合.

根据前面的定理我们有下述两个定理，可作为直接结论得到：

定理 4.3.20 对于一个给定的多项式理想 Ideal(PS) 以及任意一个基 PS, 存在一个算法，可在有限步内得到其一个良性基.

证明 事实上，根据定理 4.3.17 和构造过程，关于 PS 的方案 (W) 中最终的良序多项式集合 WAS_s 的完备化是理想 Ideal(PS) 的一个良性基. □

定理 4.3.21 一个多项式理想 Ideal(PS) 的一个良性基具有下述良性性质：

(WBP): 任意一个多项式 $P \in \mathbf{K}[X]$ 关于良性基 WB 具有形式为 (4.3.12) 的唯一标准表示.

定义 4.3.22 一个多项式 $P \in \mathbf{K}[X]$ 关于一个多项式理想的良性基 WB 的 N- 部分定义为当 P 在形式为 (4.3.12) 的标准表示中被唯一表出时的那个多项式 N.

注释 4.3.23 我们强调完备的良性基而不是其收缩的主要理由是：由方案 (W) 最终得到的自约化的多项式集合有助于得到上述的良性性质，而它的收缩不具有表示的唯一性. 在下节中我们还会看到它的其他优点.

一个例子

例 4.3.24 我们再次考虑 Czapor 及 Geddes 的例子. 为了简化计算，我们将考虑 $a = b = c = g = h = k = 1$ 的特殊情形. 这样对于给定的多项式集合 $PS = \{P_1, P_2, P_3\}$, 多项式 P_i 简化成如下形式：

$$\left.\begin{aligned} P_1 &= x^2 + y * z + d * x + 1, \\ P_2 &= y^2 + z * x + e * y + 1, \\ P_3 &= z^2 + x * y + f * z + 1. \end{aligned}\right\} \tag{4.3.15}$$

我们根据方案 (W) 由 $PS_0 = PS$ 开始逐步构造良序基 WAS_i. PS_0 的良序基 $WAS_0 = \{W_1, W_2, W_3\}$, 其中

$$W_1 = P_3, \quad W_2 = P_1, \quad W_3 = P_2 \tag{4.3.16}$$

如例 4.2.20 所示. WAS_0 中的完备的 H- 多项式共 7 个, 按降序排列, 即

$$H_1 = y*x*W_1, \quad H_2 = y*W_1, \quad H_3 = x*W_1, \quad H_4 = W_1,$$

$$H_5 = x*W_2, \quad H_6 = W_2, \quad H_7 = W_3.$$

把 H- 多项式 H 关于非乘子 i 的 N- 部分记为 $N(H/x_i)$. 根据定义可知大部分的 N- 部分是 0, 非零的 N- 部分正是下面的这些, 即

$$\begin{aligned}
N_1 &= -N(H_5/z)\\
&= -z*H_5 + H_1 - f*H_5 + x^2*H_7 + d*x*H_7 + H_7\\
&= 2*y^2*x^2 + y^2*x*d + y^2 + y*x^2*e + y*x*d*e + y*x + y*e\\
&\quad -x^3*f - x^2*d*f + x^2 + x*d - x*f + 1,\\
N_2 &= N(H_6/z)\\
&= z*H_6 - H_2 + f*H_6 - x*H_7 - d*H_7\\
&= z - 2*y^2*x - y^2*d - y*x*e - y*d*e - y\\
&\quad +x^2*f + x*d*f - x - d + f,\\
N_3 &= N(H_7/y)\\
&= y*H_7 - H_5\\
&= y^3 + y^2*e + y - x^3 - x^2*d - x,\\
N_4 &= N(H_7/z)\\
&= z*H_7 - H_3 - y*H_6 - e*H_6 + f*H_7\\
&= z + y^2*f - 2*y*x^2 - y*x*d + y*e*f - y\\
&\quad -x^2*e - x*d*e - x - e + f.
\end{aligned}$$

多项式集合 $PS_1 = WS_0 + NS_0$ 因此由 7 个多项式 W_i 及 N_j 构成. 继续下去, 我们发现, 对于 $r=6$ 多项式集合 PS_6 由下面 4 个多项式 Q_i 构成:

$$\begin{aligned}
Q_1 &= z + y^2*f - 2*y*x^2 - y*x*d + y*e*f - y\\
&\quad -x^2*e - x*d*e - x - e + f,\\
Q_2 &= y^2*d*f + y^2*f^2 + 2*y^2 + y*G_1 + G_2,\\
Q_3 &= y*x^2*G_3 + G_5,\\
Q_4 &= y*x*G_4 + G_6,
\end{aligned}$$

其中 $G_1,\cdots,G_6$ 是仅含 d,e,f 的多项式. Q_3,Q_4 的项数分别是 90 及 314. 为了使计算不过于复杂，我们进一步考虑 $f=e$ 的特殊情形，这并不会对我们前面的计算产生影响. 对于 $f=e$ 的情形，多项式 Q_i 被简化成下述形式:

$$
\begin{aligned}
Q_1 &= z+y^2*e-2*y*x^2-y*x*d+y*e^2-y\\
&\quad -x^2*e-x*d*e-x,\\
Q_2 &= y^2*d*e+y^2*e^2+2*y^2\\
&\quad +4*y*x^3+2*y*x^2*d-2*y*x^2*e\\
&\quad -y*x*d*e-y*x*e^23+2*y*x\\
&\quad +y*d*e^2+y*e^2+2*y*e\\
&\quad +2*x^3*e+2*x^2*d*e-2*x^2*e^2+2*x^2-2*x*d*e^2\\
&\quad +d*e-e^2+2,\\
Q_3 &= F_1*F_2,\\
Q_4 &= F_1*F_3.
\end{aligned}
$$

多项式 Q_3 及 Q_4 被分解成 F_i, 其中,

$$
\begin{aligned}
F_1 &= 2*x^2+x*d-x*e+2,\\
F_2 &= y*d*e-y*e^2-2*x^3-3*x^2*d-x*d^2-x-e,\\
F_3 &= 2*x^4+3*x^3*d+2*x^3*e\\
&\quad +x^2*d^2+2*x^2*d*e+x^2*e^2+x^2+x*d*e^2+2*x*e+e^2.
\end{aligned}
$$

多项式集合 $PS_6=\{Q_1,\cdots,Q_4\}$ 现在已是自约化的集合，并且可取为相应的良序基 WAS_6. 我们记其完备的 H- 多项式如下:

$$
\begin{aligned}
H_{1ij} &= x^i*y^j*Q_1, && i\le 6,\ j\le 2,\\
H_{2i} &= x^i*Q^2, && i\le 6,\\
H_{3i} &= x^i*Q_3, && i\le 4,\\
H_4 &= Q_4,
\end{aligned}
$$

那么相应非乘子的变量至多分别是

$$
\begin{aligned}
&x,y \quad 对于\ H_{1ij},\\
&x,z \quad 对于\ H_{2i},
\end{aligned}
$$

$$x, y \quad \text{对于 } H_{3i},$$
$$y, z \quad \text{对于 } H_4.$$

为了确定 N- 多项式，让我们首先考虑 $N(H_{30}/y)$, 其中 $H_{30} = Q_3$. 通过直接计算我们发现

$$(d * e + e^2 + 2) * e * (d - e) * y * H_{30}$$
$$= M_2 * Q_4 + M_3 * Q_3 + e^2 * (d - e)^2 * F_1 * Q_2,$$

其中 M_2, M_3 分别是关于 x 的二次和三次多项式. 上面方程右边出现的所有项 $x^i * Q_j$ 均是 M- 积，由此,

$$N(H_{30}/y) = 0.$$

现在考虑 $N(H_4/y)$, 其中 $H_4 = Q_4$. 把 F_2 写成 $F_2 = y * e * (d - e) - M$, 其中 M 是关于 x 的三次多项式. 然后经过形式变换我们得到

$$e * (d - e) * y * H_4 = F_3 * Q_3 + M * Q_4,$$

其中右边的所有项 $x_i * Q_4$ 均是 M- 积. 这样我们又有

$$N(H_4/y) = 0.$$

其他的 N- 多项式均为零，可由上述等式推得，或者类似地直接通过形式变换得到而几乎无需计算. 由此可知，$WAS_6 = Q_1, \cdots, Q_4$ 已是理想 Ideal(PS) 的一个良序基，其完备化即是理想的良性基.

<u>关于零点集表示的一些注释</u>

在例 3.5.32 中我们可见，即便对 Czapor 及 Geddes 例子的一般情形，即 $a, \cdots, k$ 是互不相关参数，如 3.5.110 所示，PS 的零点集可由其特征列比较容易地完全确定. 然而，如果使用良性基或等价的 Gröbner 的话，这并不是很直接的.

为了看到这一点，让我们试着在 $a = b = c = g = h = k = 1, e = f$ 的较简单的情形下由 $WAS_6 = \{Q_1, \cdots, Q_4\}$ 来确定零点集 Zero(PS) = Zero(WAS_6). 多项式 Q_3, Q_4 已被分解成 F_i. 容易看到 F_1, F_3 互素 (d, e 是互不相关的未定元), 所以 $Q_4 = 0$ 关于 x 有 6 个零点，从 $F_1 = 0$ 中得到 2 个，从 $F_3 = 0$ 得到 4 个. 在 $F_1 = 0$ 的每一零点上，Q_3 也等于零，且 $Q_2 = 0, Q_1 = 0$ 将给出

WAS_6 的两个零点. 另一方面, 对 $F_3 = 0$ 的每一个零点, 我们有 $F_1 \neq 0$. 考虑到 $F_3 = 0$, 我们得到 Q_2, F_2 关于 y 的结式为零. 因此, F_3 的这样的一个零点将被扩充到 WAS_6 的唯一的一个零点, 它由 $F_2 = 0$ 及 $Q_1 = 0$ 的确定. 最终, 我们得到 WAS_6 或 PS 的 8 个零点. 需要注意的是, 在当前情形, $Q_4 = 0$ 的每个零点可至少被扩充成 WAS_6 的一个零点. 这样我们看到, 即使在当前简单情形通过多项式集合 WAS_6 确定 $\mathrm{Zero}(PS)$ 也具有一定的复杂性. 尽管这比一般情形简单得多, 参见 [WWT18].

§4.4 良性基的性质及其与 Gröbner 基的关系

<u>前一节的回顾</u>

记号 4.4.1 除了 $\mathbf{K}, X = (x_1, \cdots, x_n)$, 等等同前面几节相同外, 我们还假定:

用 $ID = \mathrm{Ideal}(PS)$ 记一个给定的有一个基 PS 的多项式理想;

用 WB 记 ID 的一个良性基;

用 CT 记 WB 的完备的次数组集合;

用 $W_1, \cdots, W_s$ 记 WB 中按降序排列的多项式;

用 $u_i (\in CT)$ 记 W_i 的首次数组;

用 GB 记 WB 的收缩;

用 $T = \mathrm{Cont}(CT)$ 记 GB 的次数组集合;

用 $G_1, \cdots, G_r$ 记 GB 中按降序排列的多项式.

对于基 WB 和 GB, 我们有关系

$$\left.\begin{aligned} WB &= \mathrm{Comp}(GB), \\ GB &= \mathrm{Cont}(WB). \end{aligned}\right\} \tag{4.4.17}$$

我们将假定 GB 是约化的, 如果需要通过进一步约化, WB 由 $(4.4.17)_1$ 定义, 并使得 WB 仍是满足 (4.4.17) 的 ID 的一个良性基. 这一节的目的是研究 WB 和 GB 的性质. 特别地, 我们将证明, 如下面的定理 4.4.5 和 4.4.6 所示, 当 GB 是约化的时不考虑 $\mathbf{K}$ 中的非零常数因子的话, GB 正是约化的 Gröbner 基.

为此, 根据定理 4.3.13 和 4.3.21, 我们首先指出任意一个多项式 P 有唯一的标准表示

$$\left.\begin{aligned} P &= C_1 * W_1 + \cdots + C_s * W_s + N_P, \\ C_i &= \sum_{k_i} a_{ik_i} * M_{ik_i}, \end{aligned}\right\} \tag{4.4.18}$$

其中 C_i 是 M- 多项式, M_{ik_i} 是 WB 中相对于 $u_i \in CT$ 的 M 乘积, $a_{ik} \in \mathbf{K}$ 非零, k_i 遍历对应于 u_i 的乘子的各种乘积的集合, N_P 是 P 关于 WB 的 N- 部分.

对于每个 W_i, 设 t_i 是 u_i 在 CT 中具有最高序次的因子, $v_i = \frac{u_i}{t_i}$, 且 G_j 是 GB 中首次数组为 t_i 的多项式, 则

$$W_i = X^{v_i} * G_j. \tag{4.4.19}$$

合并式 (4.4.18) 中的各项重写为下面形式:

$$\begin{aligned} P \ &= D_1 * G_1 + \cdots + D_r * G_r + N_P, \\ D_j &= \sum_{(j)} C_i * X^{v_i}, \end{aligned} \tag{4.4.20}$$

其中 $\sum_{(j)}$ 对使得 t_i 与 G_j 的首次数组相同的所有 i 求和.

<u>一个多项式理想的成员问题</u>

下面的问题在理想理论中是基本的.

问题 M 以一个算法的方式或给出一个判定法则来判定多项式 P 是否是给定理想 ID 的成员, 即是否 $P \in ID$.

问题 M 最初由 Buchberger 用 Gröbner 基来解决的, 参见 [Bu3]. 我们在下面定理中通过良性基来给出成员问题的另一个解答.

定理 4.4.2 一个多项式属于理想 ID 当且仅当它是理想的良性基 WB 的一个 M- 多项式, 或它的 N- 部分为 0.

证明 显然 WB 的任意一个 M- 多项式属于理想 ID. 反之, 设 CT 是 WB 的次数组集合. 对于 CT 中任意的 u, 设 H_u 是相应的完备的多项式. 只要证明任意具有形式 $M * H_u$ 形式的乘积是一个 M 多项式即可, 其中 M 是一个单项式, u 属于 CT. 我们将通过对 $M * H_u$ 的序和单项式 M 中 x 的个数来进行归纳证明.

如果出现在单项式 M 中的每个 x_i 的 i 是 u 的一个乘子, 则 $M * H_u$ 已经是一个 M- 多项式, 无须再证. 所以假定 $M = M' * x_i$, 其中 i 是 u 的一个非乘子. 因为 WB 是理想的良性基, 相对于 u 和 i 的 N- 多项式为 0, 所以关于 $x_i * H_u$ 的 (4.4.18) 可以写为

$$x_i * H_u \ = \ a * H_w + MP,$$

其中 $w = ui$, $a\ (\in \mathbf{K}) \neq 0$, MP 是比 H_w 或 $x_i * H_u$ 序次低的 M- 多项式. 这样 $M * H_u \ = \ a * M' * H_w + M' * MP$, 其中 $M' * MP$ 比 $M * H_u$ 序次低并且 M'

比 M 有更少的 x. 根据归纳 $M' * H_w$ 和 $M' * MP$ 中的每一项是 M- 多项式, 所以 $M * H_u$ 也是. 这样定理就被证明了. □

定理 4.4.3 任意一个多项式 P 关于良性基 WB 的收缩的约化式等于 P 关于 WB 的 N- 部分.

证明 约化式 R 作为一个多项式由 $P = \sum_k C_k * G_k + R$ 决定, 其中 G_k 是 $GB = \mathrm{Cont}(WB)$ 中的多项式, C_k 也是多项式且 R 关于 GB 是约化的. 根据定理 4.4.2, $\sum_k C_k * G_k$ 是一个 M- 多项式, 所以 R 如要被证明的那样是 P 的 N- 部分. □

根据定理 4.4.3, 定理 4.4.2 可以重述为如下的另一种形式:

定理 4.4.4 一个多项式 P 属于理想 ID 当且仅当它关于理想 ID 的一个良性基 WB 的收缩的约化式为 0.

<u>良性基和 Gröbner 基的关系</u>

下面的两个定理表明一个理想的良性基和 Gröbner 基可以相互确定.

定理 4.4.5 一个多项式理想的一个良性基的收缩是此理想的一个 Gröbner 基.

证明 根据定理 4.4.2, 一个多项式属于以 WB 为良性基的理想当且仅当它关于 WB 的 N- 部分为 0, 根据定理 4.4.4, 也就是当且仅当此多项式关于 WB 的收缩 GB 的约化式为 0. 同样地对于多项式的子约化式也成立, 因为子约化式关于 GB 是约化的. 根据定义 4.2.33, 收缩 GB 是理想的一个 Gröbner 基, 如要被证明的那样. □

定理 4.4.6 一个多项式理想的一个 Gröbner 基的完备化是此理想的一个良性基.

证明 与前一个定理的证明类似. □

注释 4.4.7 定理 4.4.5 和 4.4.6 表明对一个多项式理想良性基和 Gröbner 基这两个概念实际上是等价的. 但是我们重点放在前者而不是后者是因为前者有如前面的定理 4.3.21 所述的良好性质 (WBP). 前一个概念的另一个优点可在下面的合冲的构造中看到.

<u>一个多项式理想的次数组集合</u>

下面的定义和定理源自 Macaulay 的工作. 参见 [Mac].

定义 4.4.8 一个多项式理想的 *次数组集合* 定义为属于此理想的所有多项式的首次数组的集合.

定理 4.4.9 一个多项式理想的次数组集合是其良性基的次数组集合的完

全倍数集.

证明 考虑对于任意多项式 P 的表达式 (4.4.18), 根据定理 4.4.2, P 关于一个多项式理想的一个良性基 WB 的 N- 部分 $N_p = 0$ 当且仅当 P 属于这个理想. 根据 4.1 的组分解定理, 我们看到所有乘积 $P_{ik} = M_{ik} * W_i$ 的首次数组互不相同. 所以多项式 P 的首次数组是其中具有最高序次的一个. 因为每一个 P_{ik} 都在理想中, 所以理想的次数组集合是所有这些 P_{ik} 的次数组的集合. 而后者就是基 WB 的次数组集合 CT 的完全倍数集. 这就证明了定理. □

<u>一个多项式理想基的合冲</u>

定义 4.4.10 关于一个多项式理想 $ID = \text{Ideal}(PS)$ 的一个基 $PS = \{P_1, \cdots, P_h\}$ 的 *合冲* 定义为满足下列关系的系数向量 $(g_1, \cdots, g_h)$:

$$g_1 * P_1 + \cdots + g_h * P_h = 0, \tag{4.4.21}$$

其中 $g_i \in \mathbf{K}[X]$.

定理 4.4.11 关于一个多项式理想 $ID = \text{Ideal}(PS)$ 的一个基的所有合冲的集合是多项式环 $\mathbf{K}[X]$ 上的有限维向量空间, 其与理想的基无关. 此外, 向量空间的一个有限基直接从理想的一个良性基得到.

证明 关于一个多项式理想的一个基的所有合冲的集合构成环 $\mathbf{K}[X]$ 上的一个向量空间, 这是显然的. 现在考虑同一个理想 $ID = \text{Ideal}(QS)$ 的任意一个别的基 $QS = \{Q_1, \cdots, Q_k\}$. 那么 PS 中的每个 P_i 是 Q_j 的一个线性组合, 系数在环 $\mathbf{K}[X]$ 中. 因此任意一个关于基 PS 的合冲成为一个关于基 QS 的合冲. 反之同样成立, 因此在上面的对应关系下两个基同构. 为了看到这个向量空间在 $\mathbf{K}[X]$ 上是有限维的, 让我们考虑理想 ID 的一个良性基 WB. 现在考虑基 WB 中的任意一个多项式 W_j, 其具有首次数组 $u_j \in CT$, 以及 u_j 的任意一个非乘子 k. 因为 $x_k * W_j$ 在理想 ID 中, 根据定理 4.4.2 有一个关系式

$$x_k * W_j = \sum_i M_{kji} * W_i, \tag{4.4.22}$$

这里 M_{kji} 是 WB 的所有关于 u_i 的 M- 多项式. 我们可以把上面的关系式重写为

$$\sum_i S_{kji} * W_i \;=\; 0, \tag{4.4.23}$$

那么我们看到向量 $S_{kj}=(S_{kj1},\cdots,S_{kjs})$ 构成关于基 WB 的合冲的向量空间的一个基，因此这个向量空间是有限维的.

为了看到这点，让我们考虑具有下面形式的关于 WB 的任意一个合冲方程：

$$\sum_i S_i * W_i = 0 \tag{4.4.24}$$

把 (4.4.24) 的左边记作 S. 根据定理 4.4.2 的证明，我们看到通过不断地用 (4.4.22) 或 (4.4.23) 进行约化 S 就会为 0. 因此 $S=0$ 是方程 (4.4.23) 的一个结果或者 S 是 S_{kj} 的一个线性组合，其系数为多项式，正如要证明的那样. □

<u>约化的良性基或约化的 Gröbner 基的唯一性</u>

定理 4.4.12 一个理想 ID 的约化的良性基 WB 在不考虑常数因子的情况下是唯一的.

证明 我们已经指出如何从理想 ID 的一个给定基 WB 出发用方案 (A) 和 (W) 确定理想的一个约化的自约化基 $GB=\{G_1,\cdots,G_r\}$, 其完备化是 ID 的一个约化的良性基 WB, 如果需要进一步约化的话.

现在考虑任意的另一个约化的自约化基

$$GB'=\{G'_1,\cdots,G'_s\},$$

其完备化也是一个良性基. 不失一般性，假设 GB 和 GB' 中所有的多项式都已被正规化且其首系数为 1. 我们将证明 GB' 就是 GB.

为了看到这一点让我们将 GB 和 GB' 按降序排列如下，即

$$GB: G_1 > G_2 > \cdots > G_r,$$

$$GB': G'_1 > G'_2 > \cdots > G'_s.$$

根据定理 4.4.2 和 4.4.3, 我们有 $\mathrm{Rest}(G'_1/GB)=0$ 且根据对应的约化式公式我们看到 G'_1 的首次数组是 GB 中某个多项式的首次数组的一个倍数，设为 G_i. 同理，G_i 的首次数组是 GB' 中某个多项式 G'_j 的首次数组的一个倍数. 因为 GB' 是自约化的，所以只能是 G'_j 等于 G'_1. 因此 G'_1 和 G_i 有相同的首项. 对 G_1 运用同样的推理，我们看到 G_1 和 GB' 的某个 G'_k 有相同的首单项式. 只可能有 $G_i=G_1, G'_k=G'_1$, 因此 G_1, G'_1 有相同的首项.

对 G_2 和 G'_2 运用同样的推理，我们看到它们应有相同的首单项式. 因此我们看到 GB 和 GB' 应有一样多的多项式，或 $r=s$, 且每对 G_i 和 G'_i 有相同的首单项式.

现在考虑 GB 和 GB' 中的最后的两个多项式 G_r 和 G'_r. 因为 G'_r 和 G_r 有相同的首单项式且 G'_r 关于 GB 的约化式为 0, 我们看到 G'_r 等于 G_r. 让我们考虑 G_{r-1} 和 G'_{r-1}. 因为 G'_{r-1} 相对于 GB 的约化式为 0, 我们有如下的等式:

$$G'_{r-1} = G_{r-1} + M_r,$$

其中 M_r 是从 G_r 构造的的一个 M- 多项式. 现在 G'_{r-1} 和 G_{r-1} 有相同的首单项式且 G_{r-1} 和 G'_{r-1} 中无别的单项式是 G_r 的首单项式的倍数. 根据组分解定理只能有 $M_r = 0$ 或者 G'_{r-1} 等于 G_{r-1}. 对于 GB 和 GB' 中的其他对多项式以逆序继续运用同样的推理, 我们看到每一对多项式都相等. 这样定理就被证明了. □

一个多项式理想的投影

定义 4.4.13 一个理想 $ID \subset \mathbf{K}[X]$ 在仿射空间 $A^m_{\mathbf{K}}(X_m)(m < n)$ 上的投影定义为 ID 中所有包含在多项式环 $\mathbf{K}[X_m]$ 中的多项式构成的理想, 这里 $X_m = (x_1, \cdots, x_m)$.

记号 4.4.14 用 $\mathrm{Proj}_m\, ID$ 记理想 ID 在仿射空间 $A^m_{\mathbf{K}}(X_m)$ 上的投影.

定理 4.4.15 假设 WB 是理想 $ID \subset \mathbf{K}[X]$ 的一个约化的良性基, 则多项式集合

$$WB' = WB \cap \mathbf{K}[X_m] \tag{4.4.25}$$

是理想

$$ID' = \mathrm{Proj}_m\, ID \subset \mathbf{K}[X_m]$$

的一个约化的良性基.

证明 令 CT 是 WB 的次数组集合, CT' 是 WB' 的次数组集合. 现在考虑 ID' 中任意的多项式 P. 作为 ID 中的多项式, 让我们考虑 P 并将其写成 (4.4.18) 的形式. 根据定理 4.4.2, 我们有 $N_P = 0$. 根据组分解定理, 我们看到对于 (4.4.18) 中的每一项 H_u 都有 $\mathrm{Coor}_k(u) = 0$, $k > m$. 令 $\max'(CT)$ 是从 $\max(CT)$ 中通过去掉最后 $n - m$ 个坐标得到的 m- 组. 显然 $\max(CT') \ll \max'(CT)$. 所以对于 (4.4.18) 中的每个满足 $\mathrm{Coor}_k(u) = 0 (k > m)$ 的 H_u, 使得 x_i 出现在 M_u 中的并且是关于 WB 的 u 的一个乘子的 i 也是关于 WB' 的 u 的一个乘子. 因此, P 作为 ID' 中的多项式其关于 WB' 的 N- 部分是 0. 根据定义 4.3.18, WB' 因此是理想 ID' 的一个约化的良性基. 这就完成了定理的证明. □

<u>一个素理想的投影</u>

在素理想的情形，其投影可以如下面给出的定理那样来确定：

定理 4.4.16 对与一个素理想 $ID \subset \mathbf{K}[X]$, 令 IRR 是确定不可约簇 Zero(ID) 的母点的不可约升列，使得

$$\text{Ideal}(ID) = \text{Ideal}[IRR].$$

假设 $m < n$, IRR' 是 IRR 所有只含有 X_m 而不含有 X_i 的那些多项式构成的子集，其中 $i > m$, 则

$$\text{Proj}_m \ \text{Ideal}(ID) = \text{Ideal}[IRR']. \tag{4.4.26}$$

证明 关于自然序

$$x_1 \prec \cdots \prec x_m \prec \cdots \prec x_n,$$

设 IRR 以升序表示如下：

$$A_1, \cdots, A_r.$$

设 IRR' 是 IRR 的部分升列，由 $A_1, \cdots, A_s$ 构成，其中 $s < r$. 对任意的一个多项式 $P \in \mathbf{K}[X]$, 根据定理 3.6.21, P 属于 Ideal(ID) 当且仅当

$$\text{Remdr}(P/IRR) = 0.$$

一个多项式 $P \in \mathbf{K}[X_m]$ 作为 $\mathbf{K}[X]$ 中的多项式，上述条件变成

$$\text{Remdr}(P/IRR') = 0,$$

或再一次根据定理 3.6.21, $P \in \text{Ideal}[IRR']$. 这样我们就得到 (4.4.26) 并且定理被证明. □

<u>一个多项式集合的合冲理想</u>

下面是定理 4.4.16 的一个重要的应用. 首先我们引进一些一般性的概念.

定义 4.4.17 一个多项式集合 $PS = \{P_1, \cdots, P_m\} \subset \mathbf{K}[X]$ 的一个 *合冲多项式* 定义为一个多项式 $S \equiv S(y_1, \cdots, y_m) \in \mathbf{K}[Y]$, $Y = (y_1, \cdots, y_m)$, 使得

$$S(P_1, \cdots, P_m) = 0.$$

显然所有这样的合冲多项式构成 $\mathbf{K}[Y]$ 中的一个理想.

定义 4.4.18 一个多项式集合 $PS = \{P_1, \cdots, P_m\} \subset \mathbf{K}[X]$ 的 *合冲理想* 定义为 PS 的所有 $\mathbf{K}[Y]$ 中的合冲多项式构成的 $\mathbf{K}[Y]$ 中的理想，这里 $Y = (y_1, \cdots, y_m)$.

记号 4.4.19 一个多项式集合 $PS \subset \mathbf{K}[X]$ 的合冲理想记作 Syz PS.

下面的定理解决了决定一个给定的多项式集合的合冲理想的问题.

定理 4.4.20 对于一个给定的多项式集合 $PS = \{P_1, \cdots, P_m\} \subset \mathbf{K}[X]$, 让我们考虑多项式集合 $QS = \{Q_1, \cdots, Q_m\} \subset \mathbf{K}[X, Y]$, 其中 $Q_i = y_i - P_i(X)$, $i = 1, \cdots, m$. 变量顺序为

$$y_1 \prec \cdots \prec y_m \prec x_1 \prec \cdots \prec x_n. \tag{4.4.27}$$

假设多项式集合 QS 的特征集 CS 按升序排列为

$$C_1, \cdots, C_t.$$

令 $CS' : C_1, \cdots, C_s (s < t)$ 是 CS 的部分升列, 由所有那些只含 $y_1, \cdots, y_m$ 而不含 $x_1, \cdots, x_n$ 的多项式构成, 则升列 CS 和 CS' 都是不可约的且我们有

$$\text{Syz } PS = \text{Ideal}[CS']. \tag{4.4.28}$$

证明 簇 Zero(QS) 是不可约的因为它有一个显然的母点

$$(x_1, \cdots, x_n, y_1, \cdots, y_m) = (\xi_1, \cdots, \xi_n, \eta_1, \cdots, \eta_m),$$

其中 $\xi_1, \cdots, \xi_n$ 是相互独立的超越元, $\eta_i = P_i(\xi_1, \cdots, \xi_n)$, $i = 1, \cdots, m$. 因此升列 CS 是不可约的, 表示不可约簇 Zero(QS) 的关于序 (4.4.27) 的母点. 部分升列 CS' 也是不可约的. 这个定理由定理 4.4.16 得到. □

Chou-Schelter-Yang 的一个定理

假设 IRR 是一个不可约升列, 其决定了一个不可约代数簇 Var[IRR] 和相应的理想 Ideal[IRR]. 在后面的第 5 章中我们将说明代数簇 Var[IRR] 的 Chow 基CB 或者理想 Ideal[IRR] 的一个基能直接由不可约升列 IRR 确定, 满足

$$\text{Ideal}[IRR] = \text{Ideal}(CB).$$

另一方面周咸青, Schelter 和杨劲根说明了如何通过构造 Gröbner 基直接由 IRR 确定 Ideal[IRR] 的一个基 (或者 Var[IRR] 的一个基). 参见他们合写的文章 [C-S-Y]. 我们将用良性基以下面的形式重述他们的定理:

定理 4.4.21 (Chou-Schelter-Yang) 设 IRR 是 $\mathbf{K}[X]$ 中的初式积为 IP 的一个不可约升列. 令 z 是一个新的变量其序低于 X 中所有的 x_i. 令 IRR^+ 是由 IRR 和多项式 $IP * z - 1$ 构成的特征升列, 则理想 Ideal(IRR^+) 的良性基 WB^+ 在 $A^n_{\mathbf{K}}(X)$ 上的投影是理想 Ideal[IRR] 的一个良性基 WB:

$$WB = WB^+ \cap \mathbf{K}[X].$$

证明　让我们考虑理想 Ideal$[IRR]$ 中的任意一个多项式 P. 根据定理 3.6.21 我们有 Remdr$(P/IRR)=0$. 因此存在某些非负整数 s_i, 使得

$$I_1^{s_1}*\cdots*I_r^{s_r}*P\equiv 0 \bmod_{\mathbf{K}} IRR,$$

其中 $I_1,\cdots,I_r$ 是 IRR 中多项式的初式. 令 $s=\max_i s_i$, 则上式两边同乘以 $I_1^{s-s_1}*\cdots*I_r^{s-s_r}*z^s$, 我们有

$$(IP*z)^s*P\equiv 0 \bmod_{\mathbf{K}} IRR.$$

由此可推出

$$P\equiv 0 \bmod_{\mathbf{K}} IRR^+,$$

因此 P 属于理想 Ideal(IRR^+). 因为 P 是理想 Ideal$[IRR]$ 中的任意一个多项式, 我们有

$$\text{Ideal}[IRR]=\text{Proj}_n\ \text{Ideal}(IRR^+),$$

其中 Proj_n 是指在仿射空间 $A^n_{\mathbf{K}}(X)$ 上的投影. 这样由定理 4.4.15 即可推出此定理. □

备注

注释 4.4.22　上面的大部分定理实际上是 Buchberger 和一些研究 Gröbner 基的工作者的发现. 一个多项式理想 ID 的 (约化的) 良性基仅是通常的 ID 的 (约化的)Gröbner 基的完备化. 我们所作的仅仅是像上面那样以良性基的形式重新叙述和证明这些定理. 但是这些处理和证明沿续前面几节的思路和方法, 给出关于 Gröbner 基的已知定理的另外证明, 其不同于现有的那些. 此外, 如此给出证明是为了方便地移植到微分情形, 如同 4.3 节的开始部分那样, 在那里没有相应的 Gröbner 基的概念. 进一步, 前面的处理表明 $\mathbf{K}[X]$ 中的任意一个多项式关于一个多项式理想的良性基有唯一的表示, 即方程 (4.4.18) 的形式, 这一性质比对应的在通常已知的处理方式下的约化的 Gröbner 基的表示更精确. 参见, 例如 [Wall]. 良性基的进一步的优点可从决定一个多项式理想的合冲向量空间的基的定理 4.4.11 中看到.

注释 4.4.23　这一章所发展的多项式理想的良性基理论和上一章的一个多项式集合的特征列理论的比较是个有意思的问题. 关于问题中变量的一个固定顺序, 我们首先给出多项式的一个偏序; 然后是一些特殊的多项式集合的偏序, 一种情形是自约化的集合, 另一种情形是升列; 最后是包含这些特殊类型的多项式集合在内的一般多项式集合的偏序. 我们在第一种情形通过不断

添加一些约化式，在第二种情形通过添加一些余式来降低多项式集合的序次以达到最后的目标. 最后结果的差别主要在于第一步：多项式的偏序在第一种情形是依据首多项式，在第二种情形是依据多项式的主变量. 随后的步骤则比较自然，是互相平行的.

§4.5 任意扩域上的多元多项式的因式分解和最大公因式

有理域的扩域

记号 4.5.1 考虑一个变元 x 和变元集合，

用 U 记 $(u_1, \cdots, u_d)$,

用 Y 记 $(y_1, \cdots, y_r)$,

用 X 记 $(x_1, \cdots, x_N)$.

变量次序： $u_1 \prec \cdots \prec u_d \prec y_1 \prec \cdots \prec y_r \prec x_1 \prec \cdots \prec x_N \prec x$.

不可约升列 AS 表示 $\{A_1, \cdots, A_r\} \subset \mathbf{Q}[U, Y]$, 其中

$$A_i = I_{id_i} * y_i^{d_i} + \cdots + I_{i0},$$
$$i \in I = (1, \cdots, r),\ I_{ij} \in \mathbf{Q}[U, y_1, \cdots, y_{i-1}],$$

I_{id_i} 关于 A_j 是约化的，其中 $j < i$.

用 $\mathbf{K}$ 记有理函数域 $\mathbf{Q}(U)$.

用 $\mathbf{K}^*$ 记扩域 $\mathbf{Q}(U, Y) = \mathbf{K}(Y)$, 其中 Y 通过 AS 定义.

用 T 记 $t =$ 所有的 r 元整数组 $(t_1, \cdots, t_r)$ 的集合，其中 $0 \le t_i < d_i, i \in I$. 对于 $t \in T$, 用 Y^t 记 $y_1^{t_1} * \cdots * y_r^{t_r}$.

用 $\mathbf{B}$ 记基域 $\mathbf{K}$ 或 $\mathbf{Q}$.

对于 $PS \subset \mathbf{B}[X], G \in \mathbf{B}[X]$, 用 $\mathrm{Zero}_{\mathbf{B}}(PS/G)$ 记 $\mathbf{B}^N$ 中的零点集合 $\mathrm{Zero}(PS/G) \cap \mathbf{B}^N$.

对于 $P_1, P_2 \in \mathbf{B}[x, Y]$, 用 $P_1 = P_2 \bmod_{\mathbf{B}} AS$ 记 $P_1 - P_2$ 是 AS 中 A_i 的线性组合，其系数是 $\mathbf{B}[x]$ 中的多项式.

因式分解问题和最大公因子问题

因式分解问题 F. 给定一个多项式 $F \in \mathbf{Q}[x, U, Y]$, 作为 $\mathbf{K}^*[x]$ 中的一个多项式在 $\mathbf{K}^*[x]$ 中对其因式分解.

最大公因式问题 G. 给定两个多项式 $F, G \in \mathbf{Q}[x, U, Y]$, 作为 $\mathbf{K}^*[x]$ 中的多项式确定它们的在 K^* 上的最大公因子.

上面的问题似乎很基本，但除了 Traeger, 胡森和王东明等人的一些文章，参见 [Tr], [H-W], [WDM3], 文献中很少涉及它们的一般情形. 为了看清一般问

题的要点，让我们先考虑下面的例子：

例 4.5.2 因式分解

$$F = u * x^2 - 2 * y * x - u + 1 \in \mathbf{Q}[x, u, y],$$

作为 x 的多项式，其中 y 满足方程

$$A \equiv y^2 - u = 0.$$

这个问题的解答由

$$F = u * \left(x + \frac{u - y}{u}\right) * \left(x - \frac{u + y}{u}\right) \ \mathrm{mod}_{\mathbf{K}}\ A$$

给出. 它给出了 F 在 $\mathbf{K}^*$ 上的一个因式分解. 如果我们把上面的方程写成在 $\mathbf{Q}[x, u, y]$ 中的一个方程，那么我们有

$$u * F = (u * x + u - y) * (u * x - u - y) \ \mathrm{mod}_{\mathbf{Q}}\ A,$$

F 的因式分解由于方程左边的因子 u 而变得模糊.

例 4.5.3 因式分解

$$F = x^2 - u \in \mathbf{Q}[x, u, y],$$

作为 $\mathbf{K}^*[x]$ 中的多项式，其中 y 满足方程

$$A \equiv u^3 * y^2 - 1 = 0.$$

这个问题的解答由

$$F = (x + u^2 * y) * (x - u^2 * y) \ \mathrm{mod}_{\mathbf{Q}}\ A.$$

给出. 其中因子中 u 的次数比原来 F 里的高.

上面的简单例子说明在任意扩域上的多元多项式的因式分解的复杂性 (包括确定最大公因子). 这些例子表明为了解决问题 F 和 G, 在域 $\mathbf{K} = \mathbf{Q}(U)$ 或 $\mathbf{K}(Y) = \mathbf{K}^*$ 上来考虑这两个问题要更自然一些. 这一节的目的就是通过稍加修改胡森和王东明的方法来给出另一种解决问题 F 和 G 的方法. 我们先做如下准备.

<u>一些预备知识</u>

下列事实是大家都熟悉的.

引理 4.5.4 任何一个元素 $q \in \mathbf{K}^*$ 可以唯一地表示成下面形式:

$$\sum_{t \in T} q_t * Y^t \in \mathbf{K}[Y],\ q_t \in \mathbf{K}. \tag{4.5.29}$$

根据引理 4.5.4 我们立即得到下面作为其推论的引理:

引理 4.5.5 任何一个多项式 $P \in \mathbf{K}^*[x]$ 可以唯一地表示成如下形式:

$$P = \sum_{t \in T} p_t * Y^t \in \mathbf{K}[x, Y],\ p_t \in \mathbf{K}[x] \text{ 或} \tag{4.5.30}$$

$$P = \sum_{k} p_k * x^k\ p_k \in \mathbf{K}^*, \text{ 其中} \tag{4.5.31}$$

$$p_k = \sum_{t \in T} p_{kt} * Y^t,\ p_{kt} \in \mathbf{K}. \tag{4.5.32}$$

为了避免混淆, 我们引入下列的定义和记号.

定义 4.5.6 $q \in \mathbf{K}^*$ 在 (4.5.29) 中的形式称为 q 的 *标准形式*.

定义 4.5.7 $P \in \mathbf{K}^*[x]$ 在 (4.5.31) 和 (4.5.32) 中的形式称为 P 的 *标准形式*.

记号 4.5.8 用 $[q]$ 记 $q \in \mathbf{K}^*$ 的标准形式. 用 $[P]$ 记 $P \in \mathbf{K}^*[x]$ 的标准形式.

例如, 对 A_i 中的 y_i 的幂的系数, 我们有

$$[I_{ij}] = \sum_{t \in T} I_{ijt} * Y^t,\ I_{ijt} \in \mathbf{K}. \tag{4.5.33}$$

根据这些定义和记号, 在 $\mathbf{K}^*[x]$ 中的计算可以简化为在 $\mathbf{K}[x, Y]$ 上的计算. 如下面引理所述.

引理 4.5.9 对于多项式 $P_1, P_2 \in \mathbf{K}^*[x]$, 作为 $\mathbf{K}^*[x]$ 中的多项式, $P_1 = P_2$ 等价于作为 $\mathbf{K}[x, Y]$ 中的多项式,

$$[P_1] = [P_2] \mod_{\mathbf{K}} AS. \tag{4.5.34}$$

有理系数的多变元多项式的因式分解

有许多熟知的方法用来计算系数在 $\mathbf{Q}$ 或 $\mathbf{Z}$ 上的多变元多项式的因式分解, 其效率相当高, 而且已在计算机上实现, 并有各式各样的软件包. 下面我们将描述一种因式分解的方法, 其源自胡森和王东明合作的文章 [H-W], 可以

用来解决在一般情形下的问题 F 和 G. 这个方法对变元个数 s 进行归纳. 实际上, 如果 $s=1$, 那么在 $\mathbf{Q}$ 或 $\mathbf{Z}$ 上的单变元 x 的多项式可以通过常用的方法很好地因式分解. 假设我们已经知道如何在 $s=d$ 的情形下分解, 让我们考虑 $d+1$ 个变元的一个多项式. 我们可以把其中任意一个变元作为 x, 另外的 d 个变元作为 $u_j \in U$. 问题转化为 $f \in \mathbf{Q}[x,U]$ 的因式分解. 注意根据归纳假设, 我们已经知道如何分解 $\mathbf{Q}[U]$ 中的多项式.

明白了这一点, 可以假设要分解的多项式 $f \in \mathbf{Q}[x,U]$ 如下给出:

$$f = a_n * x^n + \cdots + a_i * x^i + \cdots + a_0,\ a_i \in \mathbf{Q}[U]. \tag{4.5.35}$$

我们将看到 f 是否可以分解成 $g*h$, 其中 $g,h \in \mathbf{Q}[x,U]$ 如下给出:

$$\left.\begin{aligned} &g = x_1 * x^p + \cdots x_{p+1},\ p>0, \\ &h = x_{p+2} * x^q + \cdots + x_{p+q+2},\quad q>0, \end{aligned}\right\} \tag{4.5.36}$$

这里 $p+q=n$ 并且 $x_i(i=1,\cdots,N$, 其中 $N=n+2)$ 是 $\mathbf{Q}[U]$ 中待定的多项式. 比较方程 $f=g*h$ 两边 x 不同次幂的系数, 我们得到一个多项式方程组系统 $PS=0$, 其中 $PS \subset \mathbf{Q}[U,X]$. 把 X 看作未知变元, U 看作已知参数, 我们通过零点分解定理可以得到一个特征列 $CS_k \subset \mathbf{Q}[U,X]$, 其中初式积为 IP_k, 使得

$$\mathrm{Zero}(PS) = \bigcup_k \mathrm{Zero}(CS_k/IP_k). \tag{4.5.37}$$

假设对于某个 $k=k_0$, 特征列 CS_{k_0} 在定义 3.3.39 的意义下是不完备的. 那么根据定理 3.3.46, 存在 $u_j^0 \in \mathbf{Q}$, 记作 $CS_{k_0}^0$, $IP_{k_0}^0$ 为通过在 CS_{k_0}, IP_{k_0} 中用 u_j^0 代替 u_j 后得到的多项式. 我们有 $IP_{k_0}^0 \neq 0$ 和 $\mathrm{Zero}_{\mathbf{C}}(CS_{k_0}^0/IP_{k_0}^0)$ 是一个无限的集合. 显然我们可以找到这样的 u_j^0, 使得用 u_j^0 代替 u_j 后的 a_i, 记为 a_i^0, 有 $a_n^0 \neq 0$. 取任意一个 $\mathrm{Zero}_{\mathbf{C}}(CS_{k_0}^0/IP_{k_0}^0)$ 的复数值的解集, 我们看到它给出 $f^0 = a_n^0 * x^n + \cdots + a_0^0 \in \mathbf{Q}[x]$ 的一个分解为两个多项式 $g^0, h^0 \in \mathbf{C}[x]$ 的乘积的分解式. 由于零点集 $\mathrm{Zero}_{\mathbf{C}}(CS_{k_0}^0/IP_{k_0}^0)$ 的元素个数是无限的, 所以这样的分解式有无数个, 这显然是不可能的.

这表明因式分解 (4.5.37) 中的所有升列 CS_k 在定义 3.3.39 的意义下是完备的. 根据归纳假设和定理 3.3.47, 对于 $\mathbf{K}=\mathbf{Q}(U)$, 每一个零点集 $\mathrm{Zero}_{\mathbf{K}}(CS_k/IP_k)$ 或者是空的, 或者是有限的, 这可以通过高斯引理确定. 如果它们都是空的, 零点集 $\mathrm{Zero}_{\mathbf{K}}(PS)$ 也是空的, 那么 f 就不可能分解为 $\mathbf{Q}[U,x]$ 中的两个多项式

的积，其中 x 的次数 $p>0, q>0$，且 $p+q=n$. 否则，有限零点集 $\mathrm{Zero}_{\mathbf{K}}(PS)$ 中的每一个解都给出了这样的一种因式分解. 尝试所有可能的对 (p,q)，其中 $p>0,\ q>0,\ p+q=n$. 我们能判断 f 可不可以因式分解，并且在可分解的情形下能确定所有可能的分解式.

或者，我们可以考虑是否 f 含有 (4.5.36) 中所述的因子 g，其中关于 x 的次数为 $p,\ 0<p<n$. 实际上，如果 g 是 f 的一个因子，当且仅当作为一个变元 x 的多项式 $R\equiv \mathrm{Remdr}(f/g)=0$. 令 R 中所有 x 的幂的系数为零，我们得到一个变元 x 和 U 的多项式方程系统，这就可以和上面一样处理. 我们把上述内容以下述定理的形式总结为

定理 4.5.10 通过归纳简化为分解一个系数在 $\mathbf{Q}$ 或 $\mathbf{Z}$ 上的单变元多项式为不可约的因子的问题，有一个算法可以把任何一个系数在 $\mathbf{Q}$ 或 $\mathbf{Z}$ 上的多变元多项式分解成不可约的因子.

注释 4.5.11 另一种分解在 $\mathbf{Q}$ 或 $\mathbf{Z}$ 上的多变元多项式的方法将在第 6 章的 6.2 节给出，这种方法避免使用归纳法.

<u>解决问题 G</u>

为了确定两个已知多项式 $F,G\in\mathbf{K}^*[x]$ 的最大公因子，我们将给出一个只需求解线性多项式方程组的方法，其依赖于下面的引理.

引理 4.5.12 设 $F,G\in\mathbf{K}[x,Y]$ 关于变元 x 的次数分别为 $m,n>0$. 对于 $e\le\min(m,n)$，设 C_{m-e},D_{n-e} 是在 $\mathbf{K}[x,Y]$ 中的一对多项式，关于变元 x 的次数分别为 $m-e,n-e$，它们的系数是待定的. 考虑下面在 $\mathbf{K}^*[x]$ 中的方程:

$$D_{n-e}*F=C_{m-e}*G. \tag{4.5.38}$$

假设对所有 $e>d$，不存在这样的多项式对 $(C_{m-e},\ D_{n-e})$ 满足 (4.5.38)，而存在 $(C_{m-d},\ D_{n-d})$ 满足 (4.5.38) 的方程. 这样，我们有

$$D_{n-d}*F=C_{m-d}*G \tag{4.5.39}$$

在 $\mathbf{K}^*[x]$ 中成立. 于是 F,G 有一个最大公因子 $H\in\mathbf{K}[x,Y]$，其关于变元 x 的次数为 d，如下给出:

$$H=\left[\frac{F}{C_{m-d}}\right]=\left[\frac{G}{D_{n-d}}\right]\ \mathrm{mod}_{\mathbf{K}}\ AS. \tag{4.5.40}$$

证明 序对 (C_{m-d},D_{n-d}) 没有在 $\mathbf{K}^*$ 上的关于变元 x 的次数为正的公因子. 因为，假设存在这样的公因子 $E_c\in\mathbf{K}^*[x]$，关于变元 x 的次数 c 大于 0. 我

们可以设在 $\mathbf{K}^*[x]$ 中

$$C_{m-d-c} = \frac{C_{m-d}}{E_c},\ D_{n-d-c} = \frac{D_{n-d}}{E_c}.$$

在 (4.5.39) 的两边同时除以 E_c, 我们得到 (4.5.38) 那样的方程, 其中 $e = d+c > d$. 这和假设矛盾. 因此 C_{m-d}, D_{n-d} 没有关于变元 x 的次数为正的公因子, 这样根据 (4.5.39), 作为 $\mathbf{K}^*[x]$ 上的多项式, C_{m-d} 整除 F, D_{n-d} 整除 G. 这样我们有 (4.5.40), 如要被证明的那样. □

定理 4.5.13 存在一个算法可以通过求解线性多项式方程组来确定 $\mathbf{K}^*$ 上任意的多项式 $F, G \in \mathbf{K}[x, Y]$ 的最大公因子.

证明 设

$$\left.\begin{array}{l} F = a_m * x^m + \cdots + a_0,\ a_m \neq 0,\ a_i = \sum\limits_{t\in T} a_{it} * Y^t,\ a_{it} \in \mathbf{K} = \mathbf{Q}(U), \\ G = b_n * x^n + \cdots + b_0,\ b_n \neq 0,\ b_j = \sum\limits_{t\in T} b_{jt} * Y^t,\ b_{jt} \in \mathbf{K} = \mathbf{Q}(U), \end{array}\right\} \quad (4.5.41)$$

其中 $a_i, b_j \in \mathbf{K}[Y]$ 是已知的. 设

$$\left.\begin{array}{l} C_{m-e} = c_{m-e} * x^{m-e} + \cdots + c_0,\ c_i = \sum\limits_{t\in T} c_{it} * Y^t,\ c_{it} \in \mathbf{K} = \mathbf{Q}(U), \\ D_{n-e} = d_{n-e} * x^{n-e} + \cdots + d_0,\ d_j = \sum\limits_{t\in T} d_{jt} * Y^t,\ d_{jt} \in \mathbf{K} = \mathbf{Q}(U) \end{array}\right\} \quad (4.5.42)$$

是 $\mathbf{K}[x, Y]$ 中的两个多项式, 满足 (4.5.38), 其中 $c_{m-e} \neq 0, d_{n-e} \neq 0$. 现在 (4.5.39) 等价于

$$R \equiv \mathrm{Remdr}(C_{m-e} * G - D_{n-e} * F/AS) = 0, \quad (4.5.43)$$

其中

$$R = r_{m+n-e} * x^{m+n-e} + \cdots + r_0\ r_i = \sum_{t\in T} r_{it} * Y^t,\ r_{it} \in \mathbf{K}.$$

这样, 我们得到一个方程组

$$r_{it} = 0,\ i = 0, 1, \cdots, m+n-e,\ t \in T, \quad (4.5.44)$$

其中 r_{it} 是 c_{it}, d_{jt} 的线性函数, 其系数多项式以 a_{it}, b_{jt} 为系数. I_{ijt} 是 F, G, I_{ij} 的线性函数. 由于 c_{it}, d_{jt} 的线性形式, 容易看出系统 (4.5.44) 对任意的 e, 在

$\mathbf{Q}(U)=\mathbf{K}$ 上是否有解 (c_i,d_j). 我们现在从 $e=\min(m,n)$ 开始. 如果不存在 $\mathbf{K}=\mathbf{Q}(U)$ 的解 c_i,d_j, 我们就考虑 $e-1$ 的情形. 继续上面的步骤, 根据引理 4.5.12, 我们最终会得到要求的 F,G 的最大公因子. □

<u>求解问题 F</u>

现在通过简化为求解多项式方程组的问题, 我们在一般情形下解决问题 F.

引理 4.5.14 对于 $F\in\mathbf{K}^*[x]$ 有一个因子 $H\in\mathbf{K}^*[x]$, 关于 x 的次数大于 0 当且仅当作为 $\mathbf{K}[x,Y]$ 中的多项式,

$$\mathrm{Remdr}([F]/AS^+)=0, \tag{4.5.45}$$

其中 AS^+ 是由 AS 和多项式 $[H]$ 构成的升列.

证明 根据余式公式, 我们有对于某些多项式 Q_0, Q_i, $R\in\mathbf{K}[x,Y]$, 和 I_{id_i} 的某个幂积 IP, $i\in I$,

$$\left.\begin{aligned}&IP*I_H^s*[F]=\sum_i Q_i*A_i\ +\ Q_0*[H]\ +\ R,\\&I_H=\mathrm{Init}([H])\in\mathbf{K}[Y],\ R=\mathrm{Remdr}([F]/AS^+).\end{aligned}\right\} \tag{4.5.46}$$

首先假设 $R=0$. 那么 (4.5.46) 可以写成如下的 $\mathbf{K}^*[x]$ 中的一个方程:

$$F\ =\ \frac{Q_0}{I_H^s*IP}*H. \tag{4.5.47}$$

现在 $I_H\in\mathbf{K}[Y]$, 因此 $\frac{Q_0}{I_H^s*IP}$ 是 $\mathbf{K}^*[x]$ 中的一个多项式. 于是 (4.5.47) 表明 H 是 F 在 $\mathbf{K}^*[x]$ 中的一个因子. 反之, 假设 F 有 $\mathbf{K}^*[x]$ 中的一个因子 H. 那么对于某个多项式 $F'\in\mathbf{K}^*[x]$, 根据引理 4.5.9, 我们有

$$[F]=[F']*[H]\ \mathrm{mod}_{\mathbf{K}}\ AS,$$

这表明 $\mathrm{Remdr}([F]/AS^+)=0$, 或反过来也成立. □

定理 4.5.15 对于任意的多项式 $F\in\mathbf{K}^*[x]$,

$$[F]=a_m*x^m+\cdots a_0,\ a_i=\sum_{t\in T}a_{it}*Y^t,a_{it}\in\mathbf{K}, \tag{4.5.48}$$

有一个算法可以判断 F 在 $\mathbf{K}^*$ 上是否可约, 并且如果其可约, 可以把 F 在 $\mathbf{K}^*$ 上分解成不可约因子.

证明　设 H 是任意一个在 $\mathbf{K}^*[x]$ 上的多项式，关于 x 的次数为 d, $0 < d \leq [\frac{m}{2}]$. 设 H 的标准形式为

$$[H] = h_e * x^e + \cdots + h_0,\ h_i = \sum_{t \in T} h_{it} * Y^t,\ h_{it} \in \mathbf{K}, \tag{4.5.49}$$

$\mathbf{K}$ 上的系数 h_{it} 待定，总数为

$$N = (e+1) * d_1 * \cdots * d_r, \tag{4.5.50}$$

这些待定系数以某个确定的次序排列，以下记为 $X = (x_1, \cdots, x_N)$. 现在从一个多项式集合 $HS = \emptyset$ 和 $e = 1$ 开始，运算从 $e = 1$ 到 $e = [\frac{m}{2}]$ 如下进行.

第 1 步. 根据定理 4.5.13, F 在 $\mathbf{K}^*[x]$ 上有因子 H 的充分必要条件是

$$R \equiv \mathrm{Remdr}([F]/AS^+) = 0, \tag{4.5.51}$$

这里 AS^+ 是像以前那样通过在 AS 中添加多项式 $[H]$ 后得到的升列，基域是 $\mathbf{K} = \mathbf{Q}(U)$. 现在 R 是 $\mathbf{K}[x]$ 中的多项式，有如下形式：

$$R = r_{e-1} * x^{e-1} + \cdots + r_0,\ r_j = \sum_{t \in T} r_{jt} * Y^t, \tag{4.5.52}$$

R 已经是标准形式. 通过对余式的计算表明 $r_{jt} \in \mathbf{K}[X]$, 在 r_{jt} 中的 h_{it} 的幂次的系数是 $\mathbf{K}$ 上的关于已知的 a_{it} 和 I_{ijt} 的有理函数. (4.5.51) 成立当且仅当

$$r_{jt} = 0,\ j = 0, 1, \cdots, e-1,\ t \in T. \tag{4.5.53}$$

第 2 步. 设 $RS = \{r_{jt}\} \subset \mathbf{K}[X]$. 根据零点分解定理 (在基域 $\mathbf{K}$ 上关于不定元 X), 存在一个有限的升列 $CS_j \subset \mathbf{K}[X]$, 其中初式积 IP_j 使得

$$\mathrm{Zero}(RS) = \bigcup_j \mathrm{Zero}(CS_j/IP_j).$$

第 3 步. 像在定理 4.5.10 的证明中那样，每一个 CS_j 关于变元 X 应该是完全的，或者 $ZS_j = \mathrm{Zero}_{\mathbf{K}}(CS_j/IP_j)$ 是空的，或者是有限的，这可以根据高斯引理确定. 如果所有的 ZS_j 是空的，那么不存在具有形式 (4.5.49) 的 H 是 F 的因子. 在这种情况下，如果 $e < [\frac{m}{2}]$, 令 $e \longleftarrow e+1$, 然后转到第 1 步；如果 $e = [\frac{m}{2}]$, 返回 不可约.

第 4 步. 否则，某个 ZS_j 是非空的. 那么任意一个在这样的 ZS_j 中的零点将给出 F 的一个因子 H. 把这个因子加入 F, 然后令 $F \longleftarrow \frac{F}{H}$, 再转入第 1 步.

以上的操作会表明或者 F 是不可约的，或者是可约的，此时是多项式集合 HS 中多项式的一个乘积. □

一些例子

例 4.5.16 这个例子取自 [W-R], Ex. D17: 分解下面关于 x, y, z 的多项式

$$\begin{aligned} f = \ & x^4 + (-z+3)*x^3 + (z^3 + (y-3)*z - y^2 - 13)*x^2 \\ & +(-z^4 + (y^2 + 3*y + 15)*z + 6)*x \\ & +y*z^4 + 2*z^3 + (-y^3 - 15*y)*z - 2*y^2 - 30. \end{aligned} \tag{4.5.54}$$

解答 让我们考虑 f, 作为变元 x 的一个多项式, 把 y, z 作为 u_1, u_2. 假设我们知道如何分解两个变元 y, z 的多项式. 我们将看 f 是否可以分解成 $f = g*h$, 其中

$$\left.\begin{aligned} g = x^2 + x_1 * x + x_2, \\ h = x^2 + x_3 * x + x_4, \end{aligned}\right\} \tag{4.5.55}$$

其中 $x_i \in \mathbf{Q}[y, z] (i = 1, 2, 3, 4)$ 是待定的. 比较 x 的幂次的系数我们从 $f = g*h$ 得到一个方程组 $PS = 0$, 其中 $PS = \{P_0, P_1, P_2, P_3\}$, 具体如下:

$$\left.\begin{aligned} P_0 &= -x_4 * x_2 + z^4 * y + 2*z^3 - z*y^3 - 15*z*y - 2*y^2 - 30 \\ P_1 &= -x_4 * x_1 - x_3 * x_2 - z^4 + z*y^2 + 3*z*y + 15*z + 6 \\ P_2 &= -x_4 - x_3 * x_1 - x_2 + z^3 + z*y - 3*z - y^2 - 13 \\ P_3 &= -x_3 - x_1 - z + 3 \end{aligned}\right\} \tag{4.5.56}$$

PS 的特征列是 $CS = \{C_1, C_2, C_3, C_4\}$, 关于 $X = (x_1, \cdots, x_4)$ 是完备的，其中 $C_3 = P_3$, $C_4 = P_2$, C_2 具有一个指标集 $[16\ x_2\ 1]$. 另一方面 C_1 的指标集为 $[72\ x_1\ 6]$, 有如下形式:

$$C_1 = x_1^4 + e_3 * x_1^3 + e_2 * x_1^2 + e_1 * x_1 + e_0,\ e_i \in \mathbf{Q}[y, z].$$

现在看到 e_0 有因子 $3, z$ 和 e_0', 根据高斯引理, $C_1 = 0$ 在 $\mathbf{K} = \mathbf{Q}(y, z)$ 中唯一可能的解是 $\pm 3, \pm z, \pm e_0'$. 设 IP 是 CS 的初式积. 已经证明了 $\mathrm{Zero}(PS + \{IP\}) = \emptyset$, 而 $\mathrm{Zero}_{\mathbf{K}}(CS/IP)$ 由两个解

$$(x_1, x_2, x_3, x_4) = (-z, z*y+2, +3, z^3 - y^2 - 15)$$

或

$$= (3, z^3 - y^2 - 15, -z, z*y+2)$$

构成. 由此

$$f = (x^2 - x * z + z * y + 2) * (x^2 + 3 * x + z^3 - y^2 - 15). \tag{4.5.57}$$

另外，我们可以尝试考虑f是否有如$(4.5.55)_1$中给出的因子g. 现在 $\text{Remdr}(f/g) = 0$ 给出关于 x_1, x_2 的两个方程，其系数是 y, z 的多项式. 它们将约化为 $C_1 = 0, C_2 = 0$, 于是像上面那样我们得到 $g = x^2 - x * z + z * y + 2$ 或 $g = x^2 + 3 * x + z^3 - y^2 - 15$.

例 4.5.17 重新考虑例 4.5.3. 尝试一下因子

$$H = x + (h_1 * y + h_0),\ h_1, h_0 \in \mathbf{K}.$$

我们有

$$R \equiv \text{Remdr}(F/AS^+) = u^3 * h_1 * h_0 * y + h_1^2 + u^3 * (h_0^2 - u).$$

设 $RS = \{r_1, r_0\}$, 其中

$$r_1 = u^3 * h_1 * h_0,\ r_0 = h_1^2 + u^3 * (h_0^2 - u),$$

那么，对于序 $u \prec h_0 \prec h_1$, 我们得到

$$\text{Zero}(RS) = \text{Zero}(CS_1) + \text{Zero}(CS_2) + \text{Zero}(CS_3),$$

其中

$$\begin{aligned} CS_1 &= \{h_0, h_1 - u^2\}, \\ CS_2 &= \{h_0, h_1 + u^2\}, \\ CS_3 &= \{h_0^2 - u, h_1\}. \end{aligned}$$

升列 CS_3 没有给出 h_0, h_1 在 $\mathbf{K}$ 中的解，而 CS_1, CS_2 给出在 $\mathbf{K}$ 中可能的解. 因此有因子 $x + u^2 * y$ 和 $x - u^2 * y$, 如例 4.5.3 中所示.

例 4.5.18 确定 $\mathbf{K}^*[x]$ 中

$$F = x^2 - u,\ G = x^2 + 2 * u^2 * y + u$$

的最大公因子，其中 y 像例 4.5.3 中那样满足 $A = 0$.

解答 让我们尝试确定

$$\begin{aligned} C_1 &= x + (c_{11} * y + c_{10}), \qquad c_{1i} \in \mathbf{K}, \\ D_1 &= x + (d_{11} * y + d_{10}), \qquad d_{1i} \in \mathbf{K}. \end{aligned}$$

使得给出

$$D_1 * F = C_1 * G \text{ 在 } \mathbf{K}^*[x] \text{ 中，或}$$

$$R \equiv \mathrm{Remdr}(D_1 * F - C_1 * G/AS^+) = 0$$

其中 $R = (r_{21} * y + r_{20}) * x^2 + (r_{11} * y + r_{10}) * x + (r_{01} * y + r_{00})$ 在 $\mathbf{K}^*[x]$ 中，

$$\begin{aligned}
r_{21} &= d_{11} - c_{11} - 2 * u^2, \quad r_{20} = d_{10} - c_{10}, \\
r_{11} &= -2 * u^3 * c_{10}, \quad r_{10} = -2 * u^2 - 2 * c_{11}, \\
r_{01} &= -d_{11} - c_{11}, \quad r_{00} = -d_{10} - c_{10}.
\end{aligned}$$

方程 $r_{ij} = 0$,

$$d_{10} = c_{10} = 0,\ c_{11} = -u^2,\ d_{11} = u^2,$$

因此

$$C_1 = x - u^2 * y,\ D_1 = x + u^2 * y,$$

并且最大公因子如下给出：

$$H = \frac{F}{C_1} = \frac{G}{D_1} = x + u^2 * y \in \mathbf{K}^*[x].$$

第五章　计算代数几何中的一些问题

§5.1　实代数簇与复代数簇的一些重要特征

在本章中，符号 $\mathbf{K}$, $\mathbf{K}$ 上的 $A_{\mathbf{K}}^{n}(X)$ (具有坐标 $X = (x_1, \cdots, x_n)$) 以及 $X_k = (x_1, \cdots, x_k)$ 的含义与第 3 章和第 4 章中相同. 除非另外声明，下面所考虑的代数簇均在仿射空间 $A_{\mathbf{K}}^{n}(X)$ 中.

<u>仿射空间中的一般线性变换</u>

记号 5.1.1　令 $X' = (x'_1, \cdots, x'_n)'$;　$X'_k = (x'_1, \cdots, x'_k)'$.

$A'^{n}_{\mathbf{K}}(X')$:= 域 $\mathbf{K}$ 上的 n 维仿射空间，具有坐标为 X'.

$(\ )'$:= $A'^{n}_{\mathbf{K}}(X')$ 中的点 (关于坐标 X').

$\nu := \{v_i \mid i = 1, \cdots, r\}$:= 独立参数集.

$N := \{0, 1, \cdots, n\}$;　$N_0 := \{1, \cdots, n\}$.

u_{ij}, $i \in N_0$, $j \in N$:= 独立参数.

$\mathcal{U} := \{u_{ij} | i \in N_0, j \in N\}$.

$\mathcal{U}_0 := \{u_{ij} | i, j \in N_0\}$.

$\Delta := \{\delta_{ij} | i \in N_0, j \in N\}$.

$\Delta_0 := \{\delta_{ij} | i, j \in N_0\}$.

T: $A_{\mathbf{K}}^{n}(X) \ \rightarrow\ A'^{n}_{\mathbf{K}(\mathcal{U}_0)}(X')$, 是由下式定义的可逆线性变换:

$$x'_i = \sum_{j \in N_0} u_{ij} * x_j + u_{i0}, \quad i \in N_0. \tag{5.1.1}$$

T': $A'^{n}_{\mathbf{K}(\mathcal{U}_0)}(X') \ \rightarrow\ A_{\mathbf{K}}^{n}(X)$ 为 T 的逆线性变换.

T_0: $A_{\mathbf{K}}^{n}(X) \ \rightarrow\ A'^{n}_{\mathbf{K}(\mathcal{U}_0)}(X')$ 是由下式定义的可逆线性变换:

$$x'_i = \sum_{j \in N_0} u_{ij} * x_j, \quad i \in N_0. \tag{5.1.2}$$

T'_0: $A'^{n}_{\mathbf{K}(\mathcal{U}_0)}(X') \ \rightarrow\ A_{\mathbf{K}}^{n}(X)$ 为 T_0 的逆线性变换.

定义 5.1.2　由 (5.1.1) 所定义的 T(或 (5.1.2) 所定义的 T_0): $A_{\mathbf{K}}^{n}(X) \ \rightarrow$ $A'^{n}_{\mathbf{K}(\mathcal{U})}(X')$:= 由 $A_{\mathbf{K}}^{n}(X)$ 到 $A'^{n}_{\mathbf{K}(\mathcal{U})}(X')$ 的一般线性变换(或一般0-线性变换). T'(或 T'_0): $A'^{n}_{\mathbf{K}(\mathcal{U})}(X') \ \rightarrow\ A_{\mathbf{K}}^{n}(X)$:=T (或 T_0) 的逆变换.

域扩张的维数和特定化

命题 5.1.3 令 $\Xi=(\xi_1,\cdots,\xi_n), X^0=(x_1^0,\cdots,x_n^0)$ 是 $A_{\mathbf{K}}^n(X)$ 中的扩张点. 如果 X^0 是 Ξ 在 $\mathbf{K}$ 上的特定化, 则 X^0 也是 Ξ 在 $\mathbf{K}(\nu)$ 上的特定化.

证明 考虑任意一个多项式 $F\in\mathbf{K}(\nu)[X]$ 满足 $F(\Xi)=0, F$ 可以写成 $F=\frac{P}{Q}$ 的形式, 其中 $P\in\mathbf{K}[\nu,X], Q\in\mathbf{K}[\nu]$, 而且 P,Q 关于 ν 没有公因子, 则我们有

$$P(\nu,X)\neq 0, \text{ 而 } P(\nu,\Xi)=0.$$

再把 P 写成如下形式:

$$P(\nu,X)=\sum_I \nu^I * P_I(X),$$

其中 I 遍历非负整数有序组 $(i_1,\cdots,i_r)$ 的一个有限集,$\nu^I=v_1^{i_1}*\cdots*v_r^{i_r}$, $P_I(X)\in\mathbf{K}[X]$, 则由 $P(\nu,\Xi)=0$ 意味着有 $P_I(\Xi)=0$, 对于所有 I 成立. 由于 X^0 是 Ξ 在 $\mathbf{K}$ 上的特定化, 我们有 $P_I(X^0)=0$ 对于所有的 I 成立. 由此推出 $P(\nu,X^0)=0$. 因此, 对于每个满足 $F(\Xi)=0$ 的多项式 $F(\in\mathbf{K}(\nu)[X])$, 必有 $F(X^0)=0$. 这证明 X^0 是 Ξ 在 $\mathbf{K}(\nu)$ 上的特定化. 命题得证. □

命题 5.1.4 在域 $\mathbf{K}$ 扩张到 $\mathbf{K}(\nu)$ 时, $A_{\mathbf{K}}^n(X)$ 的扩张点 $\Xi=(\xi_1,\cdots,\xi_n)$, 维数不变, 即

$$\mathrm{Dim}_{\mathbf{K}(\nu)}\Xi=\mathrm{Dim}_{\mathbf{K}}\Xi. \tag{5.1.3}$$

证明 令 $\mathrm{Dim}_{\mathbf{K}}\Xi=d$, 则 Ξ 中的任何 $d+1$ 个元素 $\xi_{i_1},\cdots,\xi_{i_{d+1}}$ 在 $\mathbf{K}$ 上都是代数相关的, 自然在 $\mathbf{K}(\nu)$ 上也代数相关. 即

$$\mathrm{Dim}_{\mathbf{K}(\nu)}\Xi\le d. \tag{5.1.4}$$

而 $\mathrm{Dim}_{\mathbf{K}}\Xi=d$ 意味着 Ξ 中有 d 个元素, 它们在 $\mathbf{K}$ 上是代数无关的. 为简单起见, 就设这些元素是 $\xi_1,\cdots,\xi_d$. 如果 $\xi_1,\cdots,\xi_d$ 在 $\mathbf{K}(\nu)$ 上是代数相关的, 则必有某个非零的多项式 $F\in\mathbf{K}(\nu)[y_1,\cdots,y_d]$, 因而就有某个非零的多项式 $P\in\mathbf{K}[\nu,y_1,\cdots,y_d]$, 使得

$$P(\nu,y_1,\cdots,y_d)\neq 0, \quad \text{而} \quad P(\nu,\xi_1,\cdots,\xi_d)=0.$$

将 P 写成如下形式:

$$P(\nu,y_1,\cdots,y_d)=\sum_I \nu^I * P_I(y_1,\cdots,y_d),$$

其中 $I=(i_1,\cdots,i_d)$ 遍历非负整数有序数组的某个有限集, $\nu^I=v_1^{i_1}*\cdots*v_d^{i_d}$, $P_I(y_1,\cdots,y_d)\in\mathbf{K}[y_1,\cdots,y_d]$, 则我们有 $P_I(\xi_1,\cdots,\xi_d)=0$ 对所有的 I 成立. 然而,

$$P(\nu,y_1,\cdots,y_d)\neq 0$$

意味着至少有这样的一个 $I=I_0$ 使得

$$P_{I_0}(y_1,\cdots,y_d)\neq 0 \text{ 而 } P_{I_0}(\xi_1,\cdots,\xi_d)=0,$$

这证明 $\xi_1,\cdots,\xi_d$ 在 $\mathbf{K}$ 上是代数独立的, 与前面的假设矛盾. 这说明 $\xi_1,\cdots,\xi_d$ 在 $\mathbf{K}(\nu)$ 上也是代数相关的, 即有

$$\mathrm{Dim}_{\mathbf{K}(\nu)}\Xi\geq d. \tag{5.1.5}$$

由 (5.1.4) 和 (5.1.5), 我们得到

$$\mathrm{Dim}_{\mathbf{K}(\nu)}\Xi=d=\mathrm{Dim}_{\mathbf{K}}\Xi.$$

命题得证. □

<u>一般线性变换下的多项式和多项式集合</u>

定义 5.1.5　$A_{\mathbf{K}}^n(X)$ 的扩张点集 S 在一般线性 (或 0- 线性) 变换 T(或 T_0) 下的映像是指该集合的元素在变换 T(或 T^0) 下的映像的集合.

记号 5.1.6　对于 $A_{\mathbf{K}}^n(X)$ 的一个固定扩张点集 S, $T(S):=S$ 在变换 T 下 S 的映像; $T_0(S):=S$ 在变换 T_0 下 S 的映像.

定义 5.1.7　在一般线性变换 T(或一般 0- 线性变换 T_0) 下, 一个多项式

$$P(X)=P(x_1,\cdots,x_n)\in\mathbf{K}[X]$$

的映像是指多项式 $P'\in\mathbf{K}(\mathcal{U})[X']$ (或 $\mathbf{K}(\mathcal{U}_0)[X']$), 其定义为 $P'(X')=P(T'(X'))$ (或 $P'(X')=P(T_0'(X'))$).

记号 5.1.8　对于 $P\in\mathbf{K}[X]$, $T(P)$(或 $T_0(P):=P$) 在 T(或 T_0) 下的映像.

定义 5.1.9　在一般线性变换 T(一般 0- 线性变换 T_0) 下, 多项式集 $PS\subset\mathbf{K}[X]$ 的映像是指多项式集 $PS'\subset\mathbf{K}(\mathcal{U})[X']$, 其定义为

$$PS'=\{T(P)|P\in PS\}\subset\mathbf{K}(\mathcal{U})[X']$$

或

$$PS'=\{T_0(P)|P\in PS\}\subset\mathbf{K}(\mathcal{U}_0)[X'].$$

记号 5.1.10 对于 $PS \subset \mathbf{K}[X]$, $T(PS)$(或 $T_0(PS)$) $:= PS$ 在 T(或 T_0) 下的映像.

<u>一般线性变换下的特定化和维数</u>

引理 5.1.11 设 $Y^0 = (y_1^0, \cdots, y_d^0)$, 其中 $y_i^0 (i = 1, \cdots, d)$ 是 $\mathbf{K}$ 的某个扩域中的一些元素, $P_i \in \mathbf{K}[\nu, Y] (i = 1, \cdots, m)$ 是独立参数 $\nu = (v_1, \cdots, v_r)$ 与 $Y = (y_1, \cdots, y_d)$ 的一些多项式. 假定对于 $\mathbf{K}$ 中的 r 元组 $\nu^0 = (v_1^0, \cdots, v_r^0)$, $P_i(\nu, Y^0)$ $(i = 1, \cdots, m)$ 在 $\mathbf{K}(\nu)$ 上都是代数相关的. 那么, $P_i(\nu^0, Y^0)$ 在 $\mathbf{K}$ 上也是代数相关的.

证明 由于 $P_i(\nu, Y^0)$ $(i = 1, \cdots, m)$ 在 $\mathbf{K}(\nu)$ 上是代数相关的, 所以存在 $\mathbf{K}(\nu)[Z]$ 中的非零多项式, 其以 $Z = (z_1, \cdots, z_m)$ 作为独立参数, 在 $z_i = P_i(\nu, Y^0)$ 处为零. 通过去分母, 我们不妨假定存在多项式 $F(\nu, Z) \in \mathbf{K}[\nu, Z]$. 不失一般性, 我们还可进一步假定 F 没有形为 $v_i - v_i^0$ 的因子. 否则, 我们可以事先去掉这样的因子. 在这样的前提下, 我们有

$$F(\nu, Z) \neq 0, \quad \text{而 } F(\nu, \rho) = 0,$$

其中 $\rho = \{P_i(\nu, Y^0) | i = 1, \cdots, m\}$. 由于 F 没有形为 $v_i - v_i^0$ 的因子, 在最后的式子中令 $\nu = \nu^0$, 我们有

$$F(\nu^0, Z) \neq 0, \quad \text{而 } F(\nu^0, \rho^0) = 0,$$

其中 $\rho^0 = \{P_i(\nu^0, Y^0) | i = 1, \cdots, m\}$. 将 $F(\nu^0, Z)$ 写成多项式 $F^0(Z) \in \mathbf{K}[Z]$, 我们有

$$F^0(Z) \neq 0, \quad \text{而 } F^0(\rho^0) = 0,$$

这证明 $P_i(\nu^0, Y^0) (i = 1, \cdots, m)$ 在 $\mathbf{K}$ 上是代数相关的. □

命题 5.1.12 令 Ξ, X^0 是 $A_{\mathbf{K}}^n(X)$ 的扩张点, 而且 X^0 是 Ξ 在 $\mathbf{K}$ 上的特定化, 则 $T(\Xi) = \Xi'$ 与 $T(X^0) = X'^0$ 是 $A'^n_{\mathbf{K}(\mathcal{U})}(X')$ 的扩张点, 而且 $T(X^0)$ 是 X'^0 在 $\mathbf{K}(\mathcal{U})$ 上的特定化. 同样的结论对于一般 0- 线性变换也成立.

证明 考虑任意多项式 $F' \in \mathbf{K}(\mathcal{U})[X'], F'(\Xi') = 0$. 设 $F = T'(F') \in \mathbf{K}(\mathcal{U})[X]$, 则 $F(\Xi) = F'(\Xi') = 0$. 由于 X^0 是 Ξ 在 $\mathbf{K}$ 上的特定化, 根据命题 5.1.3, X^0 也是 Ξ 在 $\mathbf{K}(\mathcal{U})$ 上的特定化. 从 $F(\Xi) = 0$ 我们得 $F(X^0) = 0$. 由此推出, 对于任意满足 $F'(\Xi') = 0$ 的非零多项式 $F' \in \mathbf{K}(\mathcal{U})[X']$, 有 $F'(X'^0) = F(X^0) = 0$. 这证明 X'^0 是 Ξ' 在 $\mathbf{K}(\mathcal{U})$ 上的特定化. 关于 T_0 情形的证明完全相同. □

命题 5.1.13 仿射空间中的扩张点的维数在一般线性变换 (或者 0- 线性变换) 下不变. 更具体地说, 对于 $A^n_{\mathbf{K}(\mathcal{U})}(X)$ 中的任意扩张点 X^0, 有

$$\mathrm{Dim}_{\mathbf{K}(\mathcal{U})}T(X^0) = \mathrm{Dim}_{\mathbf{K}(\mathcal{U}_0)}T_0(X^0) = \mathrm{Dim}_{\mathbf{K}}X^0. \tag{5.1.6}$$

证明 像前一个命题的证明一样, 我们只考虑一般线性变换 T 的情形. 设 $X^0 = (x^0_1, \cdots, x^0_n)$ 在仿射空间 $A^n_{\mathbf{K}}(X)$ 中, 而它的像 $T(X^0) = X'^0 = (x'^0_1, \cdots, x'^0_n)$ 在仿射空间 $A'^n_{\mathbf{K}(\mathcal{U})}(X')$ 中. 设 $\mathrm{Dim}_{\mathbf{K}}X^0 = d$. 根据命题 5.1.4, 我们有

$$\mathrm{Dim}_{\mathbf{K}(\mathcal{U})}X^0 = \mathrm{Dim}_{\mathbf{K}}X^0 = d.$$

不失一般性, 我们假定 $x^0_1, \cdots, x^0_d$ 在 $\mathbf{K}(\mathcal{U})$ 上代数无关. 考虑如下 d 个多项式:

$$P_i(\mathcal{U}, X) = \sum_{j \in N_0} u_{ij} * x_j + u_{i0}, \quad i = 1, \cdots, d,$$

对于 $X = X^0$ 和 $\mathcal{U} = \Delta$ 我们得到

$$P_i(\Delta, X) = x^0_i, \quad i = 1, \cdots, d.$$

而 x^0_i $(i = 1, \cdots, d)$ 在 $\mathbf{K}(\mathcal{U})$ 上是代数无关的. 由引理 5.1.11, 我们知道

$$P_i(\mathcal{U}, X^0) = x'^0_i, \quad i = 1, \cdots, d,$$

在 $\mathbf{K}(\mathcal{U})$ 上也是代数无关的. 因此有

$$\mathrm{Dim}_{\mathbf{K}(\mathcal{U})}T(X^0) \geq d. \tag{5.1.7}$$

另一方面, 由命题 5.1.4 得

$$\mathrm{Dim}_{\mathbf{K}(\mathcal{U})}X^0 = d,$$

因此 X^0 中的任何 $d+1$ 个元素在 $\mathbf{K}(\mathcal{U})$ 上都是代数相关的. 由于 $T(X^0) = X'^0$ 中任何元素在 $\mathbf{K}(\mathcal{U})$ 上都是代数依赖于 X^0 的, 故 X'^0 中的任何 $d+1$ 个元素在 $\mathbf{K}(\mathcal{U})$ 上也都是代数相关的. 由此推出

$$\mathrm{Dim}_{\mathbf{K}(\mathcal{U})}T(X^0) \leq d. \tag{5.1.8}$$

由 (5.1.7) 与 (5.1.8) 我们得

$$\mathrm{Dim}_{\mathbf{K}(\mathcal{U})}T(X^0) = d = \mathrm{Dim}_{\mathbf{K}}X^0.$$

证毕. □

<u>在一般线性变换下的代数簇</u>

定理 5.1.14 仿射空间 $A^n_{\mathbf{K}}(X)$ 中的代数簇在一般线性 (或 0- 线性) 变换 $T(T_0)$ 下的映像是仿射空间 $A'^n_{\mathbf{K}(\mathcal{U})}(X')(A'^n_{\mathbf{K}(\mathcal{U}_0)}(X'))$ 的代数簇.

证明 令 $V = \mathrm{Zero}(PS)$ 是一个代数簇, 其中 $PS \subset \mathbf{K}[X]$. 对于一般线性变换 T 和它的逆变换 T', 令 $T(PS) = PS' \subset \mathbf{K}(\mathcal{U})[X']$. 直接验证我们有

$$T(\mathrm{Zero}(PS)) = \mathrm{Zero}(PS'), \tag{5.1.9}$$

因而 $T(V)$ 是 $A'^n_{\mathbf{K}(\mathcal{U})}(X')$ 中的代数簇, 即得证. T_0 情形的证明完全相同. □

定理 5.1.15 在仿射空间 $A^n_{\mathbf{K}}(X)$ 中, 以 Ξ 为母点的不可约代数簇在一般线性 (或 0- 线性) 变换 $T(T_0)$ 下的像是仿射空间 $A'^n_{\mathbf{K}(\mathcal{U})}(X')(A'^n_{\mathbf{K}(\mathcal{U}_0)}(X'))$ 中的不可约代数簇, 其母点为 $\Xi' = T(\Xi)(\Xi'_0 = T(\Xi_0))$.

证明 令 $V = \mathrm{Zero}(PS)$ 是一个不可约的代数簇, 其以 $A^n_{\mathbf{K}}(X)$ 中的扩张点 Ξ 为一个母点. 由前面的定理, 可假设 V 在 T 下的变换是代数簇 $V' = T(V) = \mathrm{Zero}(PS')$, 其中 $PS' = T(PS)$. 令 $\Xi' = T(\Xi)$, 考虑 V' 中任意点 $X'^0 = T(X^0)$, 其中 $X^0 \in V$. 由于 X^0 是 Ξ 在 $\mathbf{K}$ 上的特定化, 由命题 5.1.12, X'^0 是 Ξ' 在 $\mathbf{K}(\mathcal{U})$ 上的特定化. 由此推出 V' 是一个以 $\Xi' = T(\Xi)$ 为母点的不可约代数簇. 即得证. T_0 情形的证明完全相同. □

<u>一般线性变换下代数簇的维数</u>

定理 5.1.16 代数簇的维数在一般线性 (或 0- 线性) 变换下不变.

证明 首先考虑 V 是不可约代数簇的情形. 令 Ξ 是 V 的母点. 由定理 5.1.15, $V' = T(V)$ 是 $A'^n_{\mathbf{K}(\mathcal{U})}(X')$ 中的不可约代数簇, 而且 $\Xi' = T(\Xi)$ 是 V' 的母点. 由命题 5.1.13 我们有 $\mathrm{Dim}_{\mathbf{K}(\mathcal{U})}\Xi' = \mathrm{Dim}_{\mathbf{K}}\Xi$. 由定义 3.2.36 我们有 $\mathrm{Dim}_{\mathbf{K}(\mathcal{U})}V' = \mathrm{Dim}_{\mathbf{K}}V$, 在不可约情形定理得证. 现在考虑 V 是 $A^n_{\mathbf{K}}(X)$ 的任意代数簇. 由定理 3.2.47 或定理 3.6.29 中的 (3.6.131), V 会有一个不可缩的不可约分解, $V = \cup_i V_i$, 其中 V_i 是 V 的不可约真子簇. 由定理 5.1.16, $V' = T(V)$ 有一个不可约分解 $V' = \cup_i V'_i$, 其中每一个 $V'_i = T(V_i)$ 是不可约簇, 并且这一分解显然是不可缩的. 由定义 3.2.50, V 和 V' 的维数对应于 V_i 和 V'_i 在 $\mathbf{K}$ 和 $\mathbf{K}(\mathcal{U})$ 上的维数的极大值. 因而一般的情形可由前面特殊的不可约情形得到. 从而定理在 T 的情形完全得证. 在 T_0 的情形下, 证明完全相同. □

<u>不可约代数簇与一般超平面的交</u>

在下面我们谈到代数簇的维数时, 都是指在一个域 $\mathbf{K}$ 或它的扩张域 $\mathbf{K}(\mathcal{U})$ 或 $\mathbf{K}(\mathcal{U}_0)$ 上的维数. 如果这从上下文不难看出, 就不再另加说明.

定理 5.1.17　一个维数为 d 的不可约代数簇与一般超平面交集仍是一个不可约代数簇. 当 $d>0$ 时, 交集的维数是 $d-1$; 当 $d=0$ 时, 交集是空集.

证明　令 V 是维数为 d 的不可约代数簇. 如果 $d=0$, 则 V 由有限个点组成, 定理显然成立. 因而假定 $d>0$, $\Xi=(\xi_1,\cdots,\xi_n)$ 是 V 的一个母点, 而且 $\mathrm{Dim}_{\mathbf{K}}\Xi=d$. 令一般超平面 H_1 由下式给出:

$$u_{11}*x_1+\cdots+u_{1n}*x_n=u_{10}. \tag{5.1.10}$$

让我们考虑由 (5.1.2) 式定义的一般 0- 线性变换 T_0. 在 T_0 变换下, 超平面 H_1 将变成超平面 H_1', 其定义方程为

$$x_1'=u_{10}. \tag{5.1.11}$$

由定理 5.1.15, 点 $\Xi'=T_0(\Xi)=(\xi_1',\cdots,\xi_n')'$ 是 $V'=T_0(V)$ 的一个母点, 并且在 $\mathbf{K}(\mathcal{U}_0)$ 上具有维数 d. 假定 $\xi_{i_1}',\cdots,\xi_{i_d}'$ 是 Ξ' 中 d 个元素, 它们在 $\mathbf{K}(\mathcal{U}_0)$ 上代数无关. 于是我们可以作一个变量置换:

$$(x_1',\cdots,x_n')\to(v_1',\cdots,v_d',y_1',\cdots,y_r'),$$

其中 $r=n-d$ 而且

$$v_j'=x_{i_j}',\quad j=1,\cdots,d.$$

显然, ξ_1' 在 $\mathbf{K}(\mathcal{U}_0)$ 上超越, 所以我们可以取 $v_1'=x_1'$. 关于序

$$x_1'<\cdots<x_n',$$

令 $A'^n_{\mathbf{K}(\mathcal{U}_0)}(X')$ 的扩张点 Ξ' 的定义多项式集由下列不可约升列给出:

$$AS'\colon A_1',\cdots,A_r',\quad r=n-d,$$

这里

$$A_i'=I_i'*y_i'^{d_i'}+\text{关于}y_i'\text{的次数较低的项},\quad i=1,\cdots,r,$$

这里 A_i' 中所有 y_i' 方幂的系数都在 $\mathbf{K}(\mathcal{U}_0)[v_1',\cdots,v_d',y_1',\cdots,y_{i-1}']$ 中, 而 I_i' 在 $\mathbf{K}(\mathcal{U})[v_1',\cdots,v_d']$ 中. 现在令 A_i'' 是由多项式 A_i' 中用 u_{10} 代替 v_1' 所得的多项式, 而 A_0'' 是多项式

$$A_0''=v_1'-u_{10},$$

u_{10} 被认为 $\mathbf{K}(\mathcal{U}_0)$ 的某个扩张域中的一个固定值，则

$$AS'':\quad A_0'', A_1'', \cdots, A_r''$$

显然是一个不可约升列，代表 $A'^n_{\mathbf{K}(\mathcal{U}_0)}(X')'$ 中的一个扩张点 $\Xi'' = (\xi_1'', \cdots, \xi_n'')$. 显然，$\Xi''$ 在 $\mathbf{K}(\mathcal{U}_0)$ 上具有维数 $d-1$, 并且 Ξ'' 位于超平面 H_1' 上，因为 $\xi_1'' = u_{10}$. 用 I_i'' 记 A_i'' 的初式，I_i'' 可在 I_i' 中用 u_{10} 代替 v_1' 而得，$i = 1, \cdots, r$. 显然 $I_i''(\Xi'') \neq 0$, $i = 1, \cdots, r$, 所以 Ξ'' 在代数簇 V' 中．由此推得 Ξ'' 在 V' 与 H_1 的交中．因此，以 Ξ'' 为母点的不可约簇

$$\mathrm{Var}[AS''] = \mathrm{Spec}_{\mathbf{K}(\mathcal{U}_0)}\Xi''$$

具有维数 $d-1$, 而且全部含于 V' 与 H_1' 的交中.

反之，假设 $X''^0 = (x''^0_1, \cdots, x''^0_n)$ 是 V' 与 H_1' 交中的任意一点，则 $X''^0 \in H_1'$ 意味着 $x_1''^0 = u_{10}$. 考虑 $\mathbf{K}(\mathcal{U}_0)[X']$ 中任意的非零多项式 F, 且有 $F(\Xi'') = 0$. 由于 u_{10} 在 $\mathbf{K}(\mathcal{U}_0)$ 上超越，方程 $F(\Xi'') = 0$ 与方程 $F(\Xi') = 0$ 等价．又由于 X''^0 在 V' 中，而 V' 以 Ξ' 为母点，这可推得 $F(X''^0) = 0$. 这说明 X''^0 是 Ξ'' 在 $\mathbf{K}(\mathcal{U}_0)$ 上的特定化，因而 X''^0 在代数簇 $\mathrm{Var}[AS'']$ 中．于是

$$V' \cap H_1' = \mathrm{Var}[AS'']. \tag{5.1.12}$$

并且这是 $A'^n_{\mathbf{K}(\mathcal{U}_0)}(X')$ 中的一个不可约簇，维数是 $d-1$. 定理得证. □

<u>不可约代数簇的次数</u>

定理 5.1.18 d 维不可约代数簇与 r 维一般线性空间的交，当 $r < n-d$ 时，是空集；当 $r = n-d$ 时，是一个 0- 维的不可约代数簇，其由有限个共轭点组成.

证明 由于 r 维一般线性空间是 $n-r$ 个一般超平面的交，定理的前一部分可由上一个定理归纳地推出．定理的后一部分可由定理 3.2.41 推出. □

定义 5.1.19 d 维不可约代数簇的*次数*是指该代数簇与 $n-d$ 维一般线性空间的交中共轭点的个数.

定理 5.1.20 不可约代数簇的次数在一般线性 (或 0- 线性) 变换下不变.

证明 鉴于定理 5.1.15~5.1.18, 本定理的结论可直接由次数概念的几何意义推出. □

定理 5.1.21 0- 维不可约代数簇的次数等于该簇中共轭点的个数；不可约超曲面 $H = 0$, $H \in \mathbf{K}[X]$ 的次数等于 H 关于 X 的全次数.

证明 此结论可由定义直接推得. □

不可约代数簇的切空间

令 Zero(H) $(H \in \mathbf{K}[X])$ 是 $A_{\mathbf{K}}^{n}(X)$ 中任意超曲面, $X^0 = (x_1^0, \cdots, x_n^0)$ 是 Zero(H) 中任一点.

定义 5.1.22 Zero(H) 在点 X_0 处的*拟切空间*是指通过点 X^0 的一个线性空间, 它由下式定义:

$$\sum_{j \in N_0} \frac{\partial H}{\partial x_j}(X^0) * (x_j - x_j^0) = 0, \tag{5.1.13}$$

其中 (X^0) 指相应的偏导数在 X^0 处取值.

注释 5.1.23 在所有的偏导数于 X^0 处的取值均为零时, 拟切空间是整个仿射空间 $A_{\mathbf{K}}^{n}(X)$.

定义 5.1.24 代数簇 V 在 X^0 点的*拟切空间*是指所有包含 V 的超曲面在 X^0 点的拟切空间的交.

定义 5.1.25 不可约代数簇 V 在 X^0 点的*切空间*是指 V 在点 X^0 处的拟切空间, 如果它的维数为 $d = \mathrm{Dim}_{\mathbf{K}} V$.

注释 5.1.26 定义 5.1.24 和 5.1.25 对于 n 维代数簇 (即仿射空间 $A_{\mathbf{K}}^{n}(X)$ 本身) 无效. 在这种情形, 由定义, 拟切空间和切空间都是 $A_{\mathbf{K}}^{n}(X)$ 本身.

定理 5.1.27 维数为 d 的不可约代数簇在其母点 $\Xi = (\xi_1, \cdots, \xi_n)$ 的拟切空间的维数是 d, 并且拟切空间也是它在点 Ξ 处的切空间.

证明 如果 $d = n$, 则 $V = A_{\mathbf{K}}^{n}(X)$, 每个点都是母点, 由注释 5.1.26, 定理显然成立. 考虑 $d < n$ 的情形. 母点 Ξ 的定义升列按升序排列为

$$AS: \quad A_1, \cdots, A_r, \tag{5.1.14}$$

其中

$$\left.\begin{array}{c} A_i = I_{i0} * x_{c_i}^{d_i} + \cdots + I_{id_i}, \quad i = 1, \cdots, r, \quad r = n - d, \\ 0 < c_1 < \cdots < c_r \le n, \quad I_{ij} \in \mathbf{K}[X_{c_i - 1}]. \end{array}\right\} \tag{5.1.15}$$

让我们构造 $(r \times n)$ 的矩阵:

$$M = \left[\frac{\partial A_i}{\partial x_j}\right], \quad i = 1, \cdots, r, \quad j = 1, \cdots, n, \tag{5.1.16}$$

它的一个 $(r \times r)$ 子矩阵为

$$M_0 = \left[\frac{\partial A_i}{\partial x_{c_j}}\right], \quad i, j = 1, \cdots, r. \tag{5.1.17}$$

由于当 $j > i$ 时，$\frac{\partial A_i}{\partial x_{c_j}} = 0$, 而且 $\frac{\partial A_i}{\partial x_{c_i}} = S_i$ 是 A_i 的隔离子，有

$$\det M_0 = S_i * \cdots * S_r. \tag{5.1.18}$$

因为 S_i 关于不可约升列 AS 约化，由定理 3.6.6 在 Ξ 点 $S_i \neq 0$, 因而

$$在\ \Xi\ 点\ \det M_0 \neq 0, \tag{5.1.19}$$

进而

$$在\ \Xi\ 点\ \mathrm{Rank} M = r. \tag{5.1.20}$$

于是每个 $\mathrm{Zero}(A_i)$ 都是包含 V 的母点 Ξ 的超曲面，因而也包含整个代数簇 V. $\mathrm{Zero}(A_i)$ 在 Ξ 的拟切空间是

$$\sum_{j \in N_0} \frac{\partial A_i}{\partial x_j}(\Xi) * (x_j - \xi_j) = 0. \tag{5.1.21}$$

对于 $j = c_i$, 作为 A_i 的隔离子，由于式 (5.1.21) 中的对于 $j = c_i$ 时的偏导数在 Ξ 点不为零，拟切空间 (5.1.21) 实际上是 $\mathrm{Zero}(A_i)$ 在 Ξ 点的切空间. 这些切空间关于 x_j 的系数全体恰是矩阵 M, 由 (5.1.20), 其秩是 $r = n - d$. 这些切空间在 Ξ 点的交是一个 $n - r = d$ 维的线性空间.

现在考虑任意一个包含 V 的超曲面 $\mathrm{Zero}(H)$, 则 $\mathrm{Zero}(H)$ 包含 Ξ, 因而 $H(\Xi) = 0$. 由定理 3.6.12, 我们有

$$\mathrm{Remdr}(H/AS) = 0.$$

由第 3.3 节的余式公式 (3.3.27), 存在多项式 Q 以及 A_i 的初式 I_{i0} 的某幂次的乘积 IP_H, 使得

$$IP_H * H = \sum_i Q_i * A_i,$$

求和 $i = 1, \cdots, r$. 微分上式我们得

$$IP_H * \frac{\partial H}{\partial x_j} = -\frac{\partial IP_H}{\partial x_j} * H + \sum_i \frac{\partial Q_i}{\partial x_j} * A_i + \sum_i Q_i * \frac{\partial A_i}{\partial x_j}, \quad j \in N_0.$$

在 Ξ 点，这些方程简化为

$$IP_H(\Xi) * \frac{\partial H}{\partial x_j}(\Xi) = \sum_i Q_i(\Xi) * \frac{\partial A_i}{\partial x_j}(\Xi), \quad j \in N_0.$$

由于每个初式 I_{i0} 关于 AS 都是约化的，由定理 3.6.6 我们知 $I_{i0}(\Xi) \neq 0$, 因此 $IP_H(\Xi) \neq 0$. 在 Ξ 点，Zero(H) 的切空间是

$$\sum_{j \in N_0} \frac{\partial H}{\partial x_j}(\Xi) * (x_j - \xi_j) = 0.$$

由此看出它线性依赖于 Zero(A_i) 在 Ξ 点的这些切空间的方程. V 的拟切空间，即所有包含 V 的超曲面的拟切空间的交，恰好是由 (5.1.20) 定义的线性空间，维数是 d. V 在 Ξ 的拟切空间因而是 V 在 Ξ 点的切空间. 定理得证. □

定理 5.1.28 维数为 d 的不可约代数簇 V 在任意点的拟切空间的维数 $\geq d$.

证明 令 Ξ 是 V 的母点，则含 V 的超曲面 Zero(H) 可由 $H(\Xi) = 0$ 来刻画. 因此所有这些超曲面的多项式 H 形成一个理想 ID. 由 Hilbert 有限基定理，理想 ID 一定有有限基，设其为 $(H_1, \cdots, H_m)$. 超平面 Zero(H_k) 在 V 中任意点 $X^0 = (x_1^0, \cdots, x_n^0)$ 的拟切空间可由下式给出:

$$\sum_{j \in N_0} \frac{\partial H_k}{\partial x_j}(X^0) * (x_j - x_j^0) = 0, \quad k = 1, \cdots, m. \tag{5.1.22}$$

让我们构造诸 x_j 的 $(m \times n)$ 系数矩阵

$$M' = \left[\frac{\partial H_k}{\partial x_j}(X^0)\right], \quad k = 1, \cdots, m, \quad j = 1, \cdots, n. \tag{5.1.23}$$

对任意别的包含 V 的超曲面 Zero(H), 我们有某些多项式 Q_k 满足

$$H = \sum_k Q_k * H_k.$$

微分上式我们有

$$\frac{\partial H}{\partial x_j} = \sum_k \frac{\partial Q_k}{\partial x_j} * H_k + \sum_k Q_k * \frac{\partial H_k}{\partial x_j}.$$

在 V 的任意点 X^0, 上述方程变为

$$\frac{\partial H}{\partial x_j}(X^0) = \sum_k Q_k(X^0) * \frac{\partial H_k}{\partial x_j}(X^0).$$

因此看出 Zero(H) 的在 X^0 点的拟切空间方程线性地依赖于诸 Zero(H_k) 在 X^0 点的拟切空间的方程. 这样 V 在 X^0 点的拟切空间恰是 $(5.1.22)_k$ $(k = 1, \cdots, m)$

定义的超平面的交. 那么这个拟切空间在 X^0 点的维数等于 $n-r'(X^0)$, 其中 $r'(X^0)$ 是 (5.1.23) 中矩阵 M' 在 X^0 点的秩. 考虑 X^0 为 V 的母点 Ξ 时. 由定理 5.1.27, 我们有 $r'(\Xi)=n-d$. 由此推出对于 M' 的所有 $((n-d+1)\times(n-d+1))$ 子矩阵, 它们的行列式在母点 Ξ 将为零. 因为 V 中每个点 X^0 都是 Ξ 的特定化, 这些子矩阵的行列式在 X^0 点也等于零. 因此矩阵 M' 在点 X^0 的秩 $\leq n-d$, 进而 V 在任意点 X^0 的拟切空间的维数 $\geq d$. 定理得证. □

<u>不可约代数簇的单点与奇异点</u>

定义 5.1.29 不可约代数簇 V 中 X^0 点是*单的*指 V 的切空间在 X^0 点有定义, 或者说 V 在 X^0 点的拟切空间的维数为 $d=\mathrm{Dim}_{\mathbf{K}}V$.

定义 5.1.30 不可约代数簇 V 中的点 X^0 是*奇异的*是指 V 在 X^0 点的切空间无定义, 或者 V 在 X^0 点拟切空间的维数大于 $d=\mathrm{Dim}_{\mathbf{K}}V$.

定义 5.1.31 不可约代数簇 V 的*奇异轨迹*是指 V 的全体奇异点的集合.

定理 5.1.32 不可约代数簇 V 的奇异轨迹是 V 的真子簇.

证明 类似于定理 5.1.28 的证明, 设 $(H_1,\cdots,H_m)$ 是由使得超曲面 $\mathrm{Zero}(H)$ 包含代数簇 V 的多项式 H 构成的理想的基. 构造类似于 (5.1.23) 的矩阵 M', 则奇异点 X^0 将由 $\mathrm{Rank}M'(X^0)<n-d$ 来刻画, 其中 d 是 V 在 $\mathbf{K}$ 上的维数; 或者由 $\det M'_0(X^0)=0$ 来刻画, 其中 M'_0 遍历 M' 的所有 $((n-d)\times(n-d))$ 子矩阵. 因而, 奇轨迹是由所有这样的 $\det M'_0$ 以及 PS 中的多项式的零点集所定义的子代数簇, 其中 $\mathrm{Zero}(PS)=V$. 因为 V 的母点显然不在其中, 所以它是真子簇. □

定理 5.1.33 不可约代数簇 $V=\mathrm{Zero}(PS)$ 的奇异轨迹包含于诸真子簇 $\mathrm{Zero}(PS+S_i)$ 的并集中, 其中 S_i 是定义 V 的母点的不可约升列中多项式的隔离子.

证明 令 V 的母点的定义升列如 (5.1.14)、(5.1.15). 如果所有 A_i 的隔离子 S_i 在 V 的点 X^0 处均不为零, 那么 (5.1.17) 中的矩阵 M_0 的行列式在点 X^0 也将不为零, 所以 (5.1.15) 中矩阵 M 的秩将是 $r=n-d$, 其中 d 是 V 在 $\mathbf{K}$ 上的维数. 在 X^0 点的拟切空间的维数将不超过 d. 由定理 5.1.28, 此维数只能等于 d, 因而 X^0 将是单点, 而不是一个奇异点. 因此, 在 V 的奇异点处, 有些隔离子必为零. 定理得证. □

<u>复代数簇的拓扑</u>

现在令基域 $\mathbf{K}$ 是复数域 $\mathbf{C}$.

定义 5.1.34 对于 $PS \subset \mathbf{C}[X]$, 维数为 d 的代数簇 Zero(PS) 的 *复部分*$\mathrm{Zero}_{\mathbf{C}}(PS)$ 是指 $A^n_{\mathbf{C}}(X)$ 中的一个复代数簇, 它的复基底是 PS, 复维数是 d.

定理 5.1.35 令 Zero(PS) 是 $A^n_{\mathbf{C}}(X)$ 中一个维数为 d 的代数簇, $PS \subset \mathbf{C}[X]$. 则复簇 $\mathrm{Zero}_{\mathbf{C}}(PS)$ 是复仿射空间 $\mathbf{C}^n(X)$ 的实拓扑维数为 $2*d$ 的子空间. 而且, 在拓扑意义下, 给定一个代数簇作为 $2*d$ 维的子复形, 整个空间 $\mathbf{C}^n(X)$ 可以三角化为一个单形.

证明 参看 [Lef], Chap. VIII, Sect. 3 ; 或者 [Vdw2] Kap.IV, Anhang. □

定理 5.1.36 给定 $\mathbf{C}^n(X)$ 中一个复维数为 $d(>0)$ 的不可约复代数簇 U, 则它的奇点集 U' 是一个维数至多为 $d-1$ 的真复子簇. 在拓扑意义上, $U\backslash U'$ 是实维数为 $2*d$ 的拓扑流形, $U\backslash U'$ 的闭包是整个簇 U.

证明 证明见 [Lef], Chap. VIII, Sects 1, 2.

<u>实代数簇的拓扑</u>

这里将更详细地讨论 $\mathbf{K}=\mathbf{R}$ 的情形. 先看下面的简单例子:

例 5.1.37 在实平面 $A^2_{\mathbf{R}}(X)$ 中, 实点集 $V=\mathrm{Zero}_{\mathbf{R}}(x_1^2+x_2^2)=\mathrm{Zero}_{\mathbf{R}}(x_1,x_2)$ 仅含一个点 (0,0). 另一方面, $\mathrm{Zero}_{\mathbf{C}}(x_1^2+x_2^2)$ 是一个由两条复直线 $x_1 \pm \mathbf{i}*x_2=0$ 组成 $(\mathbf{i}=\sqrt{-1})$ 的复簇, 而实簇 $\mathrm{Zero}_{\mathbf{R}}(x_1,x_2)$ 仅含一个点 (0,0).

考虑到这些, 我们引入下面的定义.

定义 5.1.38 对于 $PS \subset \mathbf{R}[x]$, 代数簇 Zero(PS) 的 *实部分*$\mathrm{Zero}_{\mathbf{R}}(PS)$ 是指 $\mathbf{R}^n(X)$ 中的一个实簇, 其以 PS 为实基底.

定义 5.1.39 实空间 $\mathbf{R}^n(X)$ 中点集 S 的 *理想* 定义为 $\mathbf{R}[X]$ 中在 S 中的所有点上取值为 0 的多项式组成的理想.

记号 5.1.40 点集 $S \subset \mathbf{R}^n(X)$ 的理想 := Ideal(S).

由 Hilbert 基定理, Ideal(S) 总有有限基.

定义 5.1.41 对于 $\mathbf{R}^n(X)$ 中一个以 $PS \subset \mathbf{R}[X]$ 为基的实簇 $V=\mathrm{Zero}_{\mathbf{R}}(PS)$, PS 为 V 的 *实完备基*, 如果 $V=\mathrm{Zero}_{\mathbf{R}}(\mathrm{Ideal}(V))$.

例 5.1.42 对于例 5.1.37 中的实簇 V, $\{x_1,x_2\}$ 是 V 的一个完备基, 而 $\{x_1^2+x_2^2\}$ 不是 V 的完备基.

定义 5.1.43 对于 $\mathbf{R}^n(X)$ 中一个以 PS 为基的实簇 $V=\mathrm{Zero}_{\mathbf{R}}(PS)$, V 的 *复化* 是指 $\mathbf{C}(X)$ 中的复簇 $\mathrm{Zero}_{\mathbf{C}}(PS)$, 这里将 PS 看作 $\mathbf{C}[X]$ 中的多项式集.

下列关于实簇拓扑的定理都归于 Whitney. 有关证明可参考他的文章 [Whit].

定理 5.1.44 对于 $\mathbf{R}^n(X)$ 中一个以 $PS \subset \mathbf{R}[X]$ 为实完备基的实簇 $V=$

$\text{Zero}_{\mathbf{R}}(PS)$, 令 V 的复化 $V^* = \text{Zero}_{\mathbf{C}}(PS)$ 能够分解成不可约复簇 V_i^* 的不可缩的并，则每个 V_i^* 是某个实簇 V_i 的复化，且 V_i 有实的完备基 $PS_i \subset \mathbf{R}[X]$，使得 $V_i^* = \text{Zero}_{\mathbf{C}}(PS_i)$. 而且，所有 V_i 的并形成 V 的一个不可缩分解.

定理 5.1.45 $\mathbf{R}^n(X)$ 中的一个以 $PS \subset \mathbf{R}[X]$ 为基的实簇 $V = \text{Zero}_{\mathbf{R}}(PS)$ 是有限个互不相交的实拓扑流形的并，而且每一个实流形的实维数至多等于代数簇 V 在通常意义下的维数.

定义 5.1.46 定理 5.1.45 中的任何有限个实拓扑流形的集都称为实簇 V 的 Whitney 分解.

定理 5.1.47 如果 $\mathbf{R}^n(X)$ 中的一个实簇 $V = \text{Zero}_{\mathbf{R}}(PS)$ 的实基 PS 是实完备的，则在 V 的 Whitney 分解中至少有一个实的拓扑流形，它的实的拓扑维数等于代数簇 $\text{Zero}(PS)$ 的维数或实簇 V 的复化的复维数.

§5.2 代数对应和周形式

<u>一个代数对应的简单示例</u>

例 5.2.1 考虑平面 $A^n_{\mathbf{K}}(x,y)$ 上的 X 轴 L_x 与 Y 轴 L_y 以及 L_x 上的点 $(x,0)$ 或 x 与 L_y 上的点 $(0,y)$ 或 y 间的一个对应，它由下面的几何条件来定义：x,y 位于平面上过定点 (a,b) 的某一直线上，而且该点不在 L_x 或 L_y 上. 这一对应也可以由以下方程定义：

$$(x-a)*(y-b)-a*b=0,$$

它关于 x,y 是 *代数的*, 因此这一对应可以说是 *代数的*.

我们不难看出 L_x 上的点 a 在 L_y 上没有对应，而且 L_y 上的点 b 在 L_x 上也没有对应. 我们将 L_x (L_y) 转成以齐次坐标 $(x_0 : x_1)$ $((y_0 : y_1))$ 表示的射影直线 P_x (P_y), 上述用来定义对应的方程就化为

$$(x_1 - a*x_0)*(y_1 - b*y_0) - a*b*x_0*y_0 = 0,$$

则 P_x (P_y) 上的每一点毫无例外的都对应于 $P_y(P_x)$ 上的一个点. 正是基于这个原因，人们通常处理的都是 *射影* 空间的代数对应而不是仿射空间的. 尽管如此，我们仍将主要研究 *仿射* 空间中的代数对应，同时在必要的情况下我们将 *射影* 空间中的情况看作一种显然的推广.

<u>记号</u>

记号 5.2.2 $X := (x_1, \cdots, x_n)$; ${}^hX := (x_0 : x_1 : \cdots : x_n)$, 其中不是所有的 $x_i = 0$.

$Y := (y_1, \cdots, y_n)$; ${}^hY := (y_0 : y_1 : \cdots : y_n)$, 其中不是所有的 $y_i = 0$.

对于 $I = (i_1, \cdots, i_n)$, $X^I := x_1^{i_1} * \cdots * x_n^{i_n}$.

$K = (k_1, \cdots, k^m)$, $Y^K := y_1^{k_1} * \cdots * y_m^{k_m}$.

$A_{\mathbf{K}}^n(X) := \mathbf{K}$ 上的 n 维仿射空间，其中坐标为 $X = (x_1, \cdots, x_n)$.

$P_{\mathbf{K}}^n({}^hX) := A_{\mathbf{K}}^n$ 的完备的 n 维射影空间，其中 ${}^hX = (x_0 : x_1 : \cdots : x_n)$.

$A_{\mathbf{K}}^m(Y) := \mathbf{K}$ 上的 m 维仿射空间，其中 $Y = (y_1, \cdots, y_n)$.

$P_{\mathbf{K}}^m({}^hY) := A_{\mathbf{K}}^m$ 的 m 维完备的射影空间，其中 ${}^hY = (y_0 : y_1 : \cdots : y_n)$.

$\mathcal{A} :=$ 乘积空间 $A_{\mathbf{K}}^n \times A_{\mathbf{K}}^m$.

$\mathcal{P} :=$ 乘积空间 $P_{\mathbf{K}}^n \times P_{\mathbf{K}}^m$.

对于 $P \in \mathbf{K}[X]$, ${}^hP := P$ 在无穷远点 x_0 的齐次化多项式.

对于 $P \in \mathbf{K}[Y]$, ${}^hP := P$ 在无穷远点 y_0 的齐次化多项式.

对于 $P \in \mathbf{K}[X, Y]$, ${}^hP := P$ 在 X 和 Y 所对应的无穷远点 x_0, y_0 的齐次化多项式.

对于 $PS \subset \mathbf{K}[X]$, ${}^hPS := PS$ 在无穷远点 x_0 的所有齐次化多项式组成的多项式集.

对于 $PS \subset \mathbf{K}[Y]$, ${}^hPS := PS$ 在无穷远点 y_0 的所有齐次化多项式组成的多项式集.

对于 $PS \subset \mathbf{K}[X, Y]$, ${}^hPS := PS$ 在 X 与 Y 所对应的无穷远点 x_0, y_0 的所有齐次化多项式组成的多项式集.

代数对应

定义 5.2.3　$\mathcal{C}$ 是 $A_{\mathbf{K}}^n(X)$ 与 $A_{\mathbf{K}}^m(Y)$ 间的 代数对应，如果 $\mathcal{C}$ 是积空间 $\mathcal{A}$ 中的一个代数簇.

定义 5.2.4　代数对应 $\mathcal{C}$ 称为 不可约的, 如果 $\mathcal{C}$ 作为 $\mathcal{A}$ 中的代数簇是不可约的.

定义 5.2.5　$PS \subset \mathbf{K}[X, Y]$, PS 称为代数对应 $\mathcal{C}$ 的 定义多项式集, 如果 $\mathcal{C} = \mathrm{Zero}(PS)$.

定义 5.2.6　代数对应 $\mathcal{C}$ 的 射影完备化 是指 $\mathcal{P}$ 中的代数簇 $\mathrm{Zero}^h({}^hPS)$, 其中 PS 是 $\mathcal{C}$ 的定义多项式集.

除非另外声明，以下 $\mathcal{C}$ 为 $A_{\mathbf{K}}^n(X)$ 与 $A_{\mathbf{K}}^m(Y)$ 间的一个 不可约 代数对应, PS 为定义多项式集.

记号 5.2.7　用 (Ξ, Υ) 记 $\mathcal{C}$ 的母点.

定义 5.2.8　$\mathcal{C}$ 的 原像簇 是指 $A_{\mathbf{K}}^n(X)$ 中的不可约簇 $\mathrm{Spec}_{\mathbf{K}}(\Xi)$.

定义 5.2.9 $\mathcal{C}$ 的 *像簇* 是指 $A^m_{\mathbf{K}}(Y)$ 中的不可约簇 $\mathrm{Spec}_{\mathbf{K}}(\Upsilon)$.

记号 5.2.10 $\mathrm{Obj}(\mathcal{C}) :=\mathcal{C}$ 的原像簇; $Im(\mathcal{C}) := \mathcal{C}$ 的像簇.

注释 5.2.11 显然 $\mathrm{Obj}(\mathcal{C}), Im(\mathcal{C})$ 都与 $\mathcal{C}$ 中的母点 (Ξ,Υ) 的选取无关.

定理 5.2.12 如果 $(X^0,Y^0)\in\mathcal{C}$, 则 $X^0\in\mathrm{Obj}(\mathcal{C})$ 且 $Y^0\in Im(\mathcal{C})$.

证明 考虑任意多项式 $F\in\mathbf{K}[X]$, 使得 $F(\Xi)=0$. 如果 F 看成 $\mathbf{K}[X,Y]$ 中的多项式, 则 $F(\Xi,\Upsilon)=0$. 因为 (Ξ,Υ) 是 $\mathcal{C}$ 的一个母点, 我们有 $F(X^0,Y^0)=0$ 或 $F(X^0)=0$. 由于这对于任意的 $F\in\mathbf{K}[X]$ 都正确, 因此 X^0 是 Ξ 在 $\mathbf{K}$ 上的特定化, 因此 $X^0\in\mathrm{Obj}(\mathcal{C})$. 同理 $Y^0\in Im(\mathcal{C})$. □

不可约代数对应的某些特征数

记号 5.2.13 $Im_{\Xi}(\mathcal{C}) := A^{n+m}_{\mathbf{K}(\Xi)}(X,Y)$ 中的不可约簇 $\mathrm{Spec}_{\mathbf{K}(\Xi)}(\Xi,\Upsilon)$.

$\mathrm{Obj}_{\Upsilon}(\mathcal{C}) := A^{n+m}_{\mathbf{K}(\Upsilon)}(X,Y)$ 中的不可约簇 $\mathrm{Spec}_{\mathbf{K}(\Upsilon)}(\Xi,\Upsilon)$.

$a(\mathcal{C}) := \mathrm{Dim}_{\mathbf{K}}\ \mathrm{Obj}(\mathcal{C})$.

$b(\mathcal{C}) := \mathrm{Dim}_{\mathbf{K}(\Xi)}\ Im_{\Xi}(\mathcal{C})$.

$c(\mathcal{C}) := \mathrm{Dim}_{\mathbf{K}}\ Im(\mathcal{C})$.

$d(\mathcal{C}) := \mathrm{Dim}_{\mathbf{K}(\Upsilon)}\ \mathrm{Obj}_{\Upsilon}(\mathcal{C})$.

不可约代数对应的计数原理

定理 5.2.14 (计数原理) 在不可约代数对应 $\mathcal{C}$ 的特征数之间, 我们有

$$a(\mathcal{C})+b(\mathcal{C})=c(\mathcal{C})+d(\mathcal{C}). \tag{5.2.24}$$

证明 $\mathbf{K}(\Xi,\Upsilon)/\mathbf{K}$ 的超越次数可以由两种方法计算:

$$\begin{aligned}\mathrm{TrDeg}(\mathbf{K}(\Xi,\Upsilon)/\mathbf{K}) &= \mathrm{TrDeg}(\mathbf{K}(\Xi,\Upsilon)/\mathbf{K}(\Xi))+\mathrm{TrDeg}(\mathbf{K}(\Xi)/\mathbf{K})\\ &= \mathrm{TrDeg}(\mathbf{K}(\Xi,\Upsilon)/\mathbf{K}(\Upsilon))+\mathrm{TrDeg}(\mathbf{K}(\Upsilon)/\mathbf{K}).\end{aligned}$$

根据由超越次数定义的维数, 我们证明了定理. □

注释 5.2.15 代数对应的概念可以自然的推广到射影空间之间或仿射空间与射影空间的笛卡儿积. *计数原理* 经过适当修改后仍然正确. 我们将不去深究其细节, 而是给出计数原则在一般代数对应中的应用.

不可约代数簇和超曲面的交

定理 5.2.16 令 H 为 $A^n_{\mathbf{K}(a_I)}(X)$ 中由 $H(X)\equiv\sum_I a_I*X^I=0$ 定义的一般超曲面, 其中 a_I 是多项式 H 的一般系数. 那么 $A^n_{\mathbf{K}}(X)$ 中 d 维不可约代数簇 V 与 H 的交是 $A^n_{\mathbf{K}(a_I)}(X)$ 中的 $d-1$ 维不可约代数簇.

证明 假设超曲面 $H(X)=0$ 的次数为 e, 则我们有 $\max\ |I|=e$. 系数 a_I 的个数是 $E=\binom{n+e}{e}$. 令 $P^{E-1}_{\mathbf{K}}(\alpha)$ 是 $\mathbf{K}$ 上的 $E-1$ 维射影空间, 其中 α 等于

将 a_I 化为齐次坐标时的比. 现在定义一个 $A_{\mathbf{K}}^n(X)$ 与 $P_{\mathbf{K}}^{E-1}(\alpha)$ 的代数对应 $\mathcal{C}$, 它由 (X^0,α^0) 组成, 其中 X^0 属于 V, 而 $\alpha^0=(a_I^0$ 的比), 且满足 $H^0(X^0)=0$, 这里 $H^0=\sum_I a_I^0*X^I$, a_I^0 不全为零. 令 a_0 是 $H(X)$ 的常数项, 而且 a_0^0 为 $H^0(X)$ 的常数项, 这样 $a_0=-\sum_{I'} a_{I'}*X^{I'}$ 且 $a_0^0=-\sum_{I'} a_{I'}^0*X^{I'}$, 这里仅对那些 I 中的不等于 0- 整数组 $(0,\cdots,0)$ 的整数组 I' 求和, 则对应 $\mathcal{C}$ 是不可约的, 因为它有一个明显的母点 (Ξ,α^0), 其中 Ξ 是 V 的母点, 且 $\alpha^0=(a_I^0$ 的比) 为 $P_{\mathbf{K}}^{E-1}(\alpha)$ 中的点并满足 $\sum_I a_I^0*\Xi^I=0$. 因此 $a_0^0=-\sum_{I'} a_{I'}^0*X^{I'}$, 显然

$$a(\mathcal{C})=d,\ b(\mathcal{C})=E-2.$$

同时显然也有 $d(\mathcal{C})\leq d-1$, 这是因为一个一般超曲面不可能完全包含 V. 由计数原理, 我们得到 $c(\mathcal{C})\geq E-1$. 由此得到 $c(\mathcal{C})=E-1$, 这意味着像簇就是整个射影空间 $P_{\mathbf{K}}^{E-1}(\alpha)$. 再由计数原理我们有 $d(\mathcal{C})=d-1$. 这意味着 V 与一般超曲面 $\sum_I a_I*X^I=0$ 的交在 $\mathbf{K}(a_I)$ 上的是 $d-1$ 维的. 定理得证. □

现在考虑一种特殊的超曲面的情形, 即 $e=1$ 的情况. L 作为 $A_{\mathbf{K}}^n(X)$ 中 r 维的一般的线性空间是 $A_{\mathbf{K}}^n(X)$ 中的 $n-r$ 个的一般线性超平面的交, 我们可以应用上述定理在 $e=1$ 的情形成功地得到作为推论的下面的定理.

定理 5.2.17 $A_{\mathbf{K}}^n(X)$ 中域 $\mathbf{K}$ 上的 d 维不可约代数簇 V 与 $A_{\mathbf{K}}^n(X)$ 中 r 维的一般线性空间 L 的交为空集, 如果 $r<n-d$. 另一方面, 如果 $r\geq n-d$, 它们的交是扩域 $\mathbf{K}(\mathcal{L})$ 上的 $d+r-n$ 维代数簇, 其中 $\mathcal{L}$ 是决定线性空间 L 的一般参数集.

注释 5.2.18 将定理 5.2.16 和 5.2.17 与定理 5.1.17 和 5.1.18 及其证明比较, 我们很容易看到本代数对应方法的功能是十分强大的.

<u>Grassmann 簇的维数</u>

记号 5.2.19 $\mathbf{\Omega}(n,d):=P_{\mathbf{K}}^n({}^hX)$ 中的 d 维线性空间的 Grassmann 簇.

$\mathbf{\Omega}(n;0,d)$:= 复合元素 (S_0,S_d) 的 Grassmann 簇, 复合元素由点 S_0 与 $P_{\mathbf{K}}^n({}^hX)$ 中一个过 S_0 的 d 维线性空间组成.

定理 5.2.20 点集 $\mathbf{\Omega}(n,d)$ 与 $\mathbf{\Omega}(n;0,d)$ 分别为各维数足够高的射影空间上的不可约非奇异代数簇, 它们在 $\mathbf{K}$ 上的维数如下:

$$\mathrm{Dim}_{\mathbf{K}}\ \mathbf{\Omega}(n,d)=(n-d)*(d+1); \tag{5.2.25}$$

$$\mathrm{Dim}_{\mathbf{K}}\ \mathbf{\Omega}(n;0,d)=(n-d)*d+n. \tag{5.2.26}$$

证明 根据线性子空间的 Grassmann 坐标易于知道两个点集是通常的射影代数簇, 见 [H-P1], 第 VII 章. 它们是不可约的, 因为它们都有明显的母点. 在第一种情形母点由 d 维一般线性子空间组成, 在第二个种情形母点由母点及通过母点的 d 维一般线性子空间组成的对构成. 由这些变量的齐次性我们很容易地看到它们没有奇异性.

下面我们用计数原则来证明维数公式 (5.2.25) 和 (5.2.26).

令 Grassmann 簇 $\mathbf{\Omega}(n,d)$ 包含在以如上述齐次坐标 π 表示的维数 G 足够高的射影空间 $P_{\mathbf{K}}^{G}(\pi)$ 中. 考虑 $(d+1)$ 重射影空间 $P^{n,d+1}=(P_{\mathbf{K}}^{n}({}^{h}X))^{d+1}$ 和射影空间 $P_{\mathbf{K}}^{G}(\pi)$ 间的不可约代数对应 $\mathcal{C}$, 它由母点 Ξ 定义如下. 对于每一个 $j=0,1,\cdots,d$, $\Xi^{(j)}$ 是积空间 $P^{n,d+1}$ 中第 j 个分量的母点. 令 S_d 为 $P_{\mathbf{K}}^{n}(X)$ 中由 $d+1$ 个点 $\Xi^{(j)}$ 决定的 d 维线性空间, 它被看作 $P_{\mathbf{K}}^{G}(\pi)$ 中的扩充点. 定义对应 $\mathcal{C}$ 的母点由 $\Xi=((\Xi^{(0)},\Xi^{(1)},\cdots,\Xi^{(d)}),S_d)$ 给出.

现在显然 $\mathcal{C}$ 的像簇是 $P_{\mathbf{K}}^{G}(\pi)$ 中的 $\mathbf{\Omega}(n,d)$, 而且

$$a(\mathcal{C})=n*(d+1),\ b(\mathcal{C})=0,\ d(\mathcal{C})=d*(d+1).$$

由计数原理我们得到 $c(\mathcal{C})=(n-d)*(d+1)$, 或者 (5.2.25).

同理令 $P_{\mathbf{K}}^{G'}(\pi')$ 是维数 G' 足够高的射影空间, 它包含复合 Grassmann 簇 $\mathbf{\Omega}(n;0,d)$. 现在考虑如前面的 $(d+1)$ 重射影空间 $P^{n,d+1}$ 与积空间 $P_{\mathbf{K}}^{n}({}^{h}X)\times P_{\mathbf{K}}^{G'}(\pi')$ 间的不可约代数对应 $\mathcal{C}_0$, 由母点 $\Xi_0=((\Xi'(0),\Xi'^{(1)},\cdots,\Xi'^{(d)}),(\Xi'^{(0)},S_d'))$ 决定, 其中 S_d' 是通过点 $\Xi'(0)$ 的 d 维一般线性子空间, 复合元素 $(\Xi'(0),S_d')$ 被认为是在 $P_{\mathbf{K}}^{G'}(\pi')$ 中的扩充点. 显然可以看到像簇是 $\mathbf{\Omega}(n;0,d)$, 而且

$$a(\mathcal{C}_0)=n*(d+1),\ b(\mathcal{C}_0)=0,\ d(\mathcal{C}_0)=d^2.$$

由计数原理得到 $\mathrm{Dim}_{\mathbf{K}}\ \mathbf{\Omega}(n;0,d)=c(\mathcal{C}_0)=(n-d)*d+n$ 或者 (5.2.26). 因此定理完全得证. □

<u>不可约代数簇 V 的周形式</u>

以下, 我们调整下面的记号:

记号 5.2.21 $V=\mathrm{Zero}(PS)$: $=A_{\mathbf{K}}^{n}(X)$ 中的 不可约 代数簇, 对于 $PS\subset\mathbf{K}[X]$.

$\Xi=(\xi_1,\cdots,\xi_n):=V$ 的母点.

$d:=\mathrm{Dim}_{\mathbf{K}}\ V$, $r:=n-d$, $g:=Deg\ V$.

$N:=(0,1,\cdots,n)$, $N_0:=(1,\cdots,n)$.

$L := (1, \cdots, g)$.

$J := (0, 1, \cdots, d)$, $J_0 = (1, \cdots, d)$.

$U_j := (u_{j0}, u_{j1}, \cdots, u_{jn})$, $j \in J$, u_{jk} $(j \in J, k \in N)$ 为相互独立的未定元.

$(U_j, Z) := u_{j1} * z_1 + \cdots + u_{jn} * z_n + u_{j0}$, 对于 K 的任意扩域中的任意 n 次组 $Z = (z_1, \cdots, z_n)$.

$\mathcal{U}: \ = \{u_{jk} \mid j \in J, k \in N\}$; $\mathcal{U}_0 := \{u_{jk} \mid j \in J, k \in N_0\}$.

现在考虑 $\mathbf{K}(\Xi, \mathcal{U}_0)$ 中的 $d+1$ 个元素 ζ_j $(j \in J)$, 它们由下式定义:

$$\zeta_j = -\sum_{k \in N_0} u_{jk} * \xi_k, \ j \in J. \tag{5.2.27}$$

由于 Ξ 在 $\mathbf{K}$ 上是 d 维的, 故 $d+1$ 个元素 ζ_j 在 $\mathbf{K}(\mathcal{U}_0)$ 上是代数相关的. 因此对于未定元 $u_{j0}, j \in J$, 存在一个多项式

$$F(u_{00}, u_{10}, \cdots, u_{d0}) \in \mathbf{K}(\mathcal{U}_0)[u_{00}, u_{10}, \cdots, u_{d0}],$$

使得对于 $u_{j0} = \zeta_j$, $j \in J$, F 等于 0. 如此引进 u_{j0}, $j \in J$, (5.2.27) 就变成了

$$(U_j, \Xi) = 0, \ j \in J. \tag{5.2.28}$$

必要情况下我们去掉分母, 我们可以认为 F 是多项式

$$CF(\mathcal{U}) \in \mathbf{K}[\mathcal{U}], \tag{5.2.29}$$

在相差 $\mathbf{K}$ 中的非零因子下唯一. 而且, 由域的一般代数扩张理论我们有

引理 5.2.22 如果 ϕ 是 $\mathbf{K}[\mathcal{U}]$ 中的多项式, 使得 ϕ 在 $u_{j0} = \zeta_j (j \in J)$ 处为零, 则 CF 为 ϕ 的因子.

定义 5.2.23 (5.2.29) 中的多项式 CF 称为 V 的 *周形式*, 它在相差 $\mathbf{K}$ 中的非零因子下是唯一的.

<u>*周形式的另一种定义*</u>

考虑 $A^n_{\mathbf{K}}(X)$ 中的 d 个超平面 L_j $(j \in J_0)$ 定义如下:

$$(U_j, X) = 0, \ j \in J_0. \tag{5.2.30}$$

由第 5.1 节定理 5.1.18, 或本节定理 5.2.17, 定义为 $L_j (j \in J_0)$ 的交的 $(n-d)$ 维一般线性空间 S_{n-d} 与 V 相交在 g 个共轭点 $\Xi^{(l)} = (\xi^{(l)}_1, \cdots, \xi^{(l)}_n)$, $l \in L$, 则

$$P = \Pi_{l \in L} \ (U_0, \Xi^{(l)}) \ \in \mathbf{K}(\mathcal{U}_0)[U_0] \tag{5.2.31}$$

关于 $u_{00}, u_{01}, \cdots, u_{0n} \in U_0$ 是齐 g 次的. 通过对 P 乘以某一多项式 $\rho \in \mathbf{K}[\mathcal{U}_0]$, 去掉其分母, 由 P 我们得到一个多项式

$$\rho * P \in \mathbf{K}[\mathcal{U}]. \tag{5.2.32}$$

将 (5.2.31),(5.2.32) 与 (5.2.27) 比较, 并取 Ξ 为 $\Xi^{(l)}$ 中任意一个, 我们由引理 5.2.22 知 $\rho * P$ 含有 CF 作为因子. 由于 P 是 $\mathbf{K}(\mathcal{U}_l)[\mathcal{U}_l]$ 中的不可约多项式, 由此得 $\rho * P$ 与 CF 至多相差一个 $\mathbf{K}$ 中的非零因子. 因此我们有

定理 5.2.24 如果 $\Xi^{(l)} = (\xi_1^{(l)}, \cdots, \xi_n^{(l)})$ $(l \in L)$ 是一般 $(n-d)$ 维线性空间 S_{n-d} 与不可约代数簇 V 的交的 g 个共轭点, 则 V 的周形式 CF 在相差 $\mathbf{K}$ 中的一个非零因子下由 (5.2.31) 和 (5.2.32) 给出, 即

$$CF = \rho * \Pi_{l \in L}\ (U_0, \Xi^{(l)}), \tag{5.2.33}$$

其中 $\rho \in \mathbf{K}[\mathcal{U}_0]$.

由周形式 CF 的定义 5.2.31, 变量集 $U_j = (u_{j0}, u_{j1}, \cdots, u_{jn})$ 对于任意的 $j \in J$ 起着相同的作用. 由于 (5.2.33) 中的 CF 关于 U_0 中变量是 g 齐次的, 因此这对于任意变量集 $U_j (j \in J_0)$ 都是正确的. 所以我们有

定理 5.2.25 g 次不可约代数簇的周形式 $CF(\mathcal{U})$, 在每一变量集 $U_j = (u_{j0}, u_{j1}, \cdots, u_{jn})$ 中都是齐 g 次的, 其中 $j \in J$.

<u>Hodge 定理</u>

考虑 $(n-d-1)$ 维线性空间 S_{n-d-1}, 其定义方程为

$$(U_j, X) = 0,\ j \in J. \tag{5.2.34}$$

定义 5.2.26 S_{n-d-1} 的 对偶 Grassmann 坐标 定义为行列式 $(p^{(i_0 i_1 \cdots i_d)})$ 组成的集合, 其中

$$p^{(i_0 i_1 \cdots i_d)} = \begin{vmatrix} u_{0i_0} & u_{0i_1} & \cdots & u_{0i_d} \\ u_{1i_0} & u_{1i_1} & \cdots & u_{1i_d} \\ \vdots & \vdots & & \vdots \\ u_{di_0} & u_{di_1} & \cdots & u_{di_d} \end{vmatrix},\ i_j \in N.$$

现在我们有以下由 W. V. D. Hodge 所证的定理, 见 [H-P2], Chap. X.

定理 5.2.27 V 的周形式用对偶 Grassmann 坐标 $p^{(i_0 i_1 \cdots i_d)}$ 表示是一个多项式:

$$CF(\mathcal{U}) = G(p^{(i_0 i_1 \cdots i_d)}). \tag{5.2.35}$$

证明 我们设 $p^{(01\cdots d)} \neq 0$, 则 (5.2.34) 所决定的 S_{n-d-1} 同样可以由如下用 ${}^hX = (x_0 : x_1 : \cdots : x_n)$ 表示的 $d+1$ 个方程来定义:

$$p^{(01\cdots d)} * x_j + \sum_k p^{(0\cdots,j-1,k,j+1,\cdots,d)} * x_k = 0,\ j \in J, \tag{5.2.36}$$

其中和式遍历 $k \in N$ 且 $k > d$. 在得到周形式 $CF(\mathcal{U})$ 过程中, 像处理 (5.2.28) 或 (5.2.30) 一样来处理 (5.2.36), 我们得到多项式 $G(p^{(i_0 i_1 \cdots i_d)})$, 这就是所求的. □

注释 5.2.28 线性空间的对偶 Grassmann 坐标 $p^{(i_0 i_1 \cdots i_d)}$ 不是无关的, 因此, 不像形式 F 一样, 形式 G 在相差 $\mathbf{K}$ 中的非零因子下不唯一.

<u>周形式和代数对应</u>

记号 5.2.29 对于 $j \in J$, ${}^hU_j := (u_{j0} : u_{j1} : \cdots : u_{jn})$.

$\mathcal{M}$:= 乘积空间 $A^n_{\mathbf{K}}(X) \times (P^n_{\mathbf{K}}({}^hU_0) \times \cdots \times P^n_{\mathbf{K}}({}^hU_d))$.

$\mathcal{C}$:= $\mathcal{M}$ 中的代数对应, 它由集合 $(X^0, (L^0_0, L^0_1, \cdots, L^0_d))$ 组成, 其中 X^0 是 V 中的一个点, 而且 $j \in J$, L^0_j 是 $A^n_{\mathbf{K}}(X)$ 中经过此点的超平面, 由 $(U_j, X) = 0$ 和 $(U_j, X^0) = 0$ 所定义, 此超平面被认为是射影空间 $P^n_{\mathbf{K}}({}^hU_j)$ 中的一个点.

定理 5.2.30 对应 $\mathcal{C}$ 是不可约的且 $\mathcal{C}$ 的像簇由

$$CF(\mathcal{U}) = 0 \tag{5.2.37}$$

给出, 其中 CF 是 V 的周形式.

证明 因为 $\mathcal{C}$ 显然含有母点 $(\Xi, ({}^hU_0, {}^hU_1, \cdots, {}^hU_d))$, 其中 Ξ 是 V 的母点, 所以它为不可约的. 对于每一个 $j \in J$, ${}^hU_j$, 对应一个方程 $(U_j, X) = 0$ 有 $(U_j, \Xi) = 0$, 于是 $u_{j0} = -\sum_{k\in N_0} u_{jk} * \xi_k$ 定义了一个通过 Ξ 的一般超平面. 显然

$$a(\mathcal{C}) = d,\ b(\mathcal{C}) = (d+1) * (n-1),\ d(\mathcal{C}) = 0.$$

因此由计数原理我们有

$$c(\mathcal{C}) = (d+1) * n - 1.$$

因此像簇 $\mathcal{C}$ 是积空间 $P^n_{\mathbf{K}}({}^hU_0) \times \cdots \times P^n_{\mathbf{K}}({}^hU_d)$ 中的超曲面, 由以下方程定义:

$$F_0(U_0, U_1, \cdots, U_d) = 0,$$

其中 F_0 是 $\mathbf{K}[\mathcal{U}]$ 中的不可约多项式, 它在每一个变量集 $U_j = (u_{j0}, \cdots, u_{jn}) (j \in J)$ 中都是齐次的.

令由 $(U_j, X) = 0$ $(j \in J_0)$ 定义的 $n-d$ 维线性空间与 V 相交在 g 个母点 $\Xi^{(l)}, l \in L$, 则 $F_0(U_0, U_1, \cdots, U_d) = 0$ 当且仅当对于一个 $l \in L$, 有 $(U_j, \Xi^{(l)}) = 0$, $j \in J$. 由引理 5.2.22 知 F_0 能被周形式 CF 整除. 由于 F_0 不可约, 它与 CF 在 $\mathbf{K}$ 中至多相差一个非零因子. 这就证明了定理. □

从上述定理最后部分的证明, 我们可以得到作为推论的下面的定理:

定理 5.2.31 $A^n_{\mathbf{K}}(X)$ 中由 $(U_j, X) = 0$ $(j \in J_0)$ 定义的 $d+1$ 个超平面组成的集合, 与 d 维不可约簇 V 有一个公共点当且仅当 $F_0(U_0, U_1, \cdots, U_d) = 0$, 或 $CF(\mathcal{U}) = 0$, 其中 CF 是 V 的周形式.

不可约代数簇的周基

定理 5.2.32 点 Ξ^0 属于 d 维不可约代数簇 V 当且仅当任意通过点 Ξ^0 的一般线性空间都与 V 有公共点.

证明 首先设 Ξ^0 不属于 V. 我们取 V 中的任意点, 且令 S_{n-1} 为通过 Ξ^0 但不通过那一点的一般超平面, 则 S_{n-1} 与 V 相交在一个代数簇, 它的每一不可约分支的维数小于或等于 $d-1$. 现在在每一分支上任取一点, 令 S_{n-2} 是维数为 $n-2$ 的通过点 Ξ^0 包含在 S_{n-1} 中且不包含所选的点的一般线性空间. 同样 S_{n-2} 与 V 相交在一个代数簇, 它的每一个不可约分支的维数都小于等于 $d-2$. 同样的方法进行下去, 我们得到一个通过点 Ξ^0 且维数为 $n-d$ 的一般线性空间 S_{n-d}, 它与 V 相交于至多有限个点组成的集合. 现在取任一个通过 Ξ^0 但不通过这些点的超平面, 则这一超平面与 S_{n-d} 相交在一个 $n-d-1$ 维的线性空间 S_{n-d-1}, 它通过 Ξ^0, 但与 V 无交点.

反之, 设 Ξ^0 属于 V, 则任意的 $n-d-1$ 维线性空间都与 V 有公共点, 例如 Ξ^0. 这就证明了定理. □

引理 5.2.33 一个一般超平面, 通过点

$$Z = (z_1, \cdots, z_n),$$

则其形式为 $(U, X) = 0$, 其中 U 是矩阵积

$$U = {}^h Z \cdot S, \quad {}^h Z = (1, z_1, \cdots, z_n),$$

且 S 是一个 $(n+1)$ 阶斜对称矩阵, s_{ik} 是独立变元, 对于 $i < k$, 而 $s_{ki} = -s_{ik}$, $i, k \in N$.

证明 这可以利用 Grassmann 坐标得到证明. □

记号 5.2.34 对于 $j \in J$, $S^{(j)} = (s^{(j)}_{ik})(i, k \in N)$ 代表 $(n+1)$ 阶斜对称矩阵, $s^{(j)}_{ik}$ 是独立变元, 对于 $i < k$, 而 $s^{(j)}_{ki} = -s^{(j)}_{ik}$, 其中 $i, k \in N$.

对于 $j \in J$, $U_j^0 = (u_{j0}^0, u_{j1}^0, \cdots, u_{jn}^0) :=$ 矩阵积 ${}^hZ \cdot S^{(j)}$.

$\mathcal{U}^0 := \{u_{ji}^0\}$ 组成的集合，　$i \in N$, $j \in J$.

$T :=$ 非负整数 $(t_{ik}^{(j)} \mid j \in J,\ i,k \in N,\ i < k)$ 形成的整数组.

对于 $t = (t_{ik}^{(j)}) \in T$, $S^t := (s_{ik}^{(j)})^{t_{ik}^{(j)}}$ 的积，其中 $j \in J$, $i,k \in N$, $i < k$.

定理 5.2.35　点 $Z = (z_1, \cdots, z_n)$ 属于 V 当且仅当方程

$$CF(\mathcal{U}^0) = 0 \tag{5.2.38}$$

对 $s_{ik}^{(j)}$, $i < k$, 恒成立，其中 CF 是 V 的周形式.

证明　如果 $d+1$ 个通过点 $Z = (z_1, \cdots, z_n)$ 的超平面，用 $(U_j^0, X) = 0 (j \in J)$ 表示，由引理 5.2.33 和定理 5.2.31, 5.2.32 可推出本定理. □

作为推论我们有下面定理，它从 V 的周形式重新得到了 V 的定义方程.

定理 5.2.36　令

$$CF(\mathcal{U}^0) = \sum_{t \in T} C_t * S^t, \tag{5.2.39}$$

则

$$V = \mathrm{Zero}(CB), \tag{5.2.40}$$

其中

$$CB = \{C_t \mid t \in T\} \subset \mathbf{K}[X]. \tag{5.2.41}$$

因此 V 可由下面方程定义:

$$CB = 0,$$

或

$$V = \mathrm{Zero}(CB). \tag{5.2.42}$$

定义 5.2.37　$CB :=$ 不可约簇 V 的 *周基*.

定义 5.2.38　不可约簇 V 的周形式 CF 的系数按一定的顺序排列的比称为簇 V 的 *周坐标*.

注释 5.2.39　对于固定的 d, g, 我们考虑 d 维 g 次的不可约簇的周坐标作为某射影空间的一个点. 这些点将会定义射影空间中的一个不可约代数簇，称为对应于固定值 d 与 g 的 *周簇*. 来自于周形式的这些概念允许我们不仅能对代数簇的性质进行研究，也能对代数簇形成的代数系统进行研究，这些我们就不涉及了. 见 [Ch-VdW], [VdW2], [H-P2].

注释 5.2.40 上述引入的周形式，周基，周坐标及与它们关系密切的内容在 [Ch-VdW] 和 [VdW2] 中给出，它是在考虑 [H-P2], Chap. X 并经过适当修改后得到的. 但是这种处理是比较复杂的，而且，有例子可以显示即使在最简单的情况下，这种方法也不太有效. 而且基中会出现多余的多项式. 看起来需要其他方法来简化.

§5.3 具有任意奇性的不可约代数簇的陈类与陈数

混合元素的 Grassmannian

在本节中，除另外声明外，$\mathbf{K}$ 总是表示特征为 0 的固定的域.

定义 5.3.1 $P^n_{\mathbf{K}}$ 中混合元素 $\mathrm{GR}(n;0,d)$ 的 Grassmannian 是指混合元素 (L_0, L_d) 的集合，其中 L_0 是 $P^n_{\mathbf{K}}$ 中的一个点，L_d 是 $P^n_{\mathbf{K}}$ 中过点 L_0 的一个维数为 d 的线性子空间.

定理 5.3.2 $\mathrm{GR}(n;0,d)$ 是 $\mathbf{K}$ 上的一个非奇异代数簇，其维数为

$$D = (n-d) * (d+1) + d, \tag{5.3.43}$$

它可以在维数 N 充分大的射影空间中实现.

证明 可参见上一节.

因此，除非另外声明，非奇异簇 $\mathrm{GR}(n;0,d)$ 将以记号 G 表示，其中 n, d 固定. 我们假设它是 $P^N_{\mathbf{K}}$ 的一个子簇，其中 N 充分大.

Grassmannian $\mathrm{GR}(n;0,d) = G$ 的 Schubert 圈

考虑射影空间 $P^n_{\mathbf{K}}$ 中的一个由维数为 i 的线性子空间 S_i 组成的序列 $\mathcal{S}$ 满足:

$$\mathcal{S}: S_0 \subset S_1 \subset \cdots \subset S_n = P^n_{\mathbf{K}}. \tag{5.3.44}$$

定义 5.3.3 相对于序列 $\mathcal{S}$ 具有 Ehresmann 符号 $\begin{bmatrix} a_0 & & & \\ b_0 & b_1 & \cdots & b_d \end{bmatrix}$，其中

$$0 \le a_0 \le n,\ 0 \le b_0 < b_1 < \cdots < b_d \le n \tag{5.3.45}$$

的 Schubert圈 是指 G 的一个由混合元素 (L_0, L_d) 组成的子簇，其中

$$\mathrm{Dim}_{\mathbf{K}}\ (L_d \cap S_{b_j}) \ge j, \quad j = 0, 1, \cdots, d. \tag{5.3.46}$$

特别地，当 $j = 0$ 时，(5.3.46) 意味着 $L_0 \in S_{a_0}$.

在下面，所有的 Schubert 圈均是相对于 (5.3.44) 中某一固定的序列 $\mathcal{S}$ 而言的. 因此，“相对于 $\mathcal{S}$”将被省略，除非另外声明.

记号 5.3.4　Ehresmann 符号中 (i,j)(其中 $i<j$) 是指从 i 到 j 的连续整数的序列.

定义 5.3.5　基本 Schubert 圈 是指具有 Ehresmann 符号 $\begin{bmatrix} a_0 & & & \\ b_0 & b_1 & \cdots & b_d \end{bmatrix}$ 的 Schubert 圈，其中 a_0 等于某一个 b_j. 特别地，我们有

$$\mathrm{GR}(n;0,d)=\begin{bmatrix} n \\ (n-d,n) \end{bmatrix}. \tag{5.3.47}$$

定义 5.3.6　基本 Schubert 圈的 对偶 $\begin{bmatrix} b_i & & \\ b_0 & \cdots & b_d \end{bmatrix}$ 是指基本 Schubert 圈 $\begin{bmatrix} n-b_i & & \\ n-b_d & \cdots & n-b_0 \end{bmatrix}$.

记号 5.3.7　$\begin{bmatrix} b_i & & \\ b_0 & \cdots & b_d \end{bmatrix}$ 的对偶：$=\delta\begin{bmatrix} b_i & & \\ b_0 & \cdots & b_d \end{bmatrix}$：

$$\delta\begin{bmatrix} b_i & & \\ b_0 & \cdots & b_d \end{bmatrix}=\begin{bmatrix} n-b_i & & \\ n-b_d & \cdots & n-b_0 \end{bmatrix}. \tag{5.3.48}$$

注释 5.3.8　显然，一个基本 Schubert 圈对偶的对偶是其本身.

定义 5.3.9　Schubert 圈的 余维数 定义为其对偶的维数.

记号 5.3.10　具有 Ehresmann 符号 E 的 Schubert 圈的 维数 或 余维数 $:=\mathrm{Dim}_{\mathbf{K}}\,E$ 或 $\mathrm{Codim}_{\mathbf{K}}\,E$.

定理 5.3.11　基本 Schubert 圈

$$E=\begin{bmatrix} b_i & & & \\ b_0 & b_1 & \cdots & b_d \end{bmatrix} \tag{5.3.49}$$

的维数由

$$\mathrm{Dim}_{\mathbf{K}}\,E=\mathrm{Codim}_{\mathbf{K}}\,\mathrm{Dual}\,E=\sum_j (b_j-j)+b_i \tag{5.3.50}$$

给出，这里求和从 $j=0$ 到 $j=d$.

证明是初等的，这里省略.

代数簇的代数等价群与周环

给定某一个射影空间 $P_{\mathbf{K}}^{N}$ 中维数为 d_V 的不可约代数簇 V. 根据周形式的理论，包含于 V (或者 圈) 中有固定维数 r 的不可约子簇的形式代数和可以赋予一个等价关系. 因此，所有 代数等价类 的全体被赋予自然的加法结构，就成为一个 Abel 群. 该群称为 V 的维数为 r 或者余维数为 $d_V - r$ 的 代数等价群, 并记之为 $\mathrm{Alg}_r(V)$. 特别地，我们有

$$\mathrm{Alg}_0(V) \approx \mathbf{Z}. \tag{5.3.51}$$

因此我们可以将 $\mathrm{Alg}_0(V)$ 与 $\mathbf{Z}$ 等同起来. 所有的这些从 $r=0$ 到 $r=d_V$ 的群的直和记为 $A_*(V)$. 如果 V 是非奇异的，则相交运算诱导出 $A_*(V)$ 中的乘法 $*$, 使之成为具有单位元的环，满足

$$\mathrm{Alg}_r(V) * \mathrm{Alg}_s(V) \subset \mathrm{Alg}_{r+s-d_V}(V), \quad \text{对于 } r+s \geq d_V,$$

或

$$\mathrm{Codim}_{\mathbf{K}}\ (A * B) = \mathrm{Codim}_{\mathbf{K}}\ A + \mathrm{Codim}_{\mathbf{K}}\ B, \quad \text{对于} A, B \in \mathrm{Alg}_*(V). \tag{5.3.52}$$

我们省略上述事实的证明细节，它们可以从文献或者代数几何的相关论文中找到，例如 [H-P2].

定义 5.3.12 如 (5.3.52) 中确定的 $\mathbf{K}$ 上维数为 d 的非奇异簇 V 的环称为 非奇异簇 V 的 相交环 或 周环.

$\mathrm{GR}(n;0,d)$ 的代数等价群

定理 5.3.13 (Ehresmann) 当 $\mathbf{K}=\mathbf{C}$ 时，基本 Schubert 圈的内域构成了作为拓扑流形的 $\mathrm{GR}(n;0,d)$ 的一个胞腔剖分.

该证明可参见 Ehresmann [Eh] 的原文.

定理 5.3.14 相对于同 $\mathcal{S}$ 一样的不同序列具有相同 Ehresmann 符号

$$\begin{bmatrix} b_i & & & \\ b_0 & b_1 & \cdots & b_d \end{bmatrix}$$

的基本 Schubert 圈属于同一代数等价类.

证明 对任意两个序列 $\mathcal{S}, \mathcal{S}'$, 存在 $P_{\mathbf{K}}^{n}$ 的某一射影变换，将 $\mathcal{S}$ 的线性子空间变为 $\mathcal{S}'$ 的线性子空间. 于是将相应于 $\mathcal{S}$ 的 Schubert 圈变换为相应于 $\mathcal{S}'$ 具有相同符号的 Schubert 圈，从而它们是代数等价的. □

定义 5.3.15 符号 (5.3.49) 的 Ehresmann 类是指基本 Schubert 圈 (5.3.49) 确定的代数等价类.

记号 5.3.16 为简化记号，符号 (5.3.49) 的代数等价类与 Schubert 圈 (5.3.49) 将用同一个符号 (5.3.49) 表示. 在这样定义之后，就不会发生误解. 定义类的对偶所诱导的运算符记为 δ_*.

定理 5.3.17 (周炜良) Ehresmann 类构成了 Grassmannian $\mathrm{GR}(n;0,d)$ 的代数等价群 $\mathrm{Alg}_*(\mathrm{GR}(n;0,d))$ 的一组加性基.

证明参见周炜良的原文 [Chow1,2], 该文包含了很多一般性的内容.

$\mathrm{GR}(n;0,d)$ 的相交环或周环

由于 $G=\mathrm{GR}(n;0,d)$ 是非奇异代数簇，所以在其代数等价类之间可以定义相交，从而使 $\mathrm{Alg}_*(G)$ 成为一个环，G 的 周环.

定理 5.3.18 余维数小于或者等于 d 的 $\mathrm{GR}(n;0,d)$ 的周环，在余维数 1 时由类 δ_*P 生成，在余维数 $h(0\le h\le d)$ 时由类 δ_*Q_h 生成，其中

$$\begin{aligned} P &= \begin{bmatrix} 1 \\ (0,d) \end{bmatrix}, \\ Q_h &= \begin{bmatrix} 0 & \\ (0,d-1), & d+h \end{bmatrix}. \end{aligned} \tag{5.3.53}$$

特别地，我们有

$$\delta_*\begin{bmatrix} i & & & \\ (0,i), & b_{i+1}, & \cdots, & b_d \end{bmatrix} = \delta_*\begin{bmatrix} 0 & & & \\ (0,i), & b_{i+1}, & \cdots, & b_d \end{bmatrix} * (\delta_*P)^i, \tag{5.3.54}$$

$$\delta_*\begin{bmatrix} 0 & & \\ a_0, & \cdots, & a_d \end{bmatrix} * \delta_*\begin{bmatrix} 0 & & \\ b_0, & \cdots, & b_d \end{bmatrix} = \sum_c \delta_*\begin{bmatrix} 0 & & \\ c_0, & \cdots, & c_d \end{bmatrix}. \tag{5.3.55}$$

在公式 (5.3.55) 中，求和是对所有的 $c=(c_0,\cdots,c_d)$ 取的，使得对于通常的 Grassmann 簇 $\boldsymbol{\Omega}(n,d)$, 我们有相交公式

$$\delta_*\begin{bmatrix} a_0,\cdots,a_d \end{bmatrix} * \delta_*\begin{bmatrix} b_0,\cdots,b_d \end{bmatrix} = \sum_c \delta_*\begin{bmatrix} 0,\cdots,c_d \end{bmatrix}. \tag{5.3.56}$$

证明 该证明是初等的，故在此不给出. (5.3.56) 的显式表示可以参见 [H-P2], (Chap. XIV, Sect. 6), 该公式可以由 Pieri 与 Giambelli 的著名公式导出.

具有特殊兴趣的代数等价类

除了类 P, Q_h 及其对偶外，我们还对下面的类特别感兴趣：

定义 5.3.19 Gamkrelidze-Todd 类 定义为

$$GT_{st} = \begin{bmatrix} s-t & \\ (0, d-t), & (d-t+2, d+1) \end{bmatrix} \in \mathrm{Alg}_s(\mathrm{GR}(n;0,d)), \quad \text{其中 } 0 \le t \le s \le d. \tag{5.3.57}$$

定义 5.3.20 陈类 定义为

$$Ch_s = \sum_t (-1)^t * \binom{d-t+1}{d-s+1} * GT_{st} \in \mathrm{Alg}_s(\mathrm{GR}(n;0,d)), \quad \text{其中 } 0 \le s \le d, \quad \text{求和遍历} 0 \le t \le s. \tag{5.3.58}$$

记号 5.3.21 正数 p 的分划 π是指

$$\pi = (p_1, \cdots, p_s),$$

其中

$$0 < p_1 \le \cdots \le p_s, \ p_1 + \cdots + p_s = p.$$

定义 5.3.22 分划 π 的陈类 是

$$Ch_\pi = \delta_*(\delta_*\ Ch_{p_1} * \cdots * \delta_*\ Ch_{p_s}) \in \mathrm{Alg}_p(\mathrm{GR}(n;0,d)). \tag{5.3.59}$$

从定理 5.3.18, 我们有下面的关系式：

$$\left.\begin{aligned}
\delta_*Ch_1 &= (d+1) * \delta_*P - \delta_*Q_1. \\
\delta_*Ch_2 &= \binom{d+1}{2} * (\delta_*P)^2 - d * \delta_*P * \delta_*Q_1 + (\delta_*Q_1)^2 - \delta_*Q_2. \\
\delta_*Ch_3 &= \binom{d+1}{3} * (\delta_*P)^3 - \binom{d}{2} * (\delta_*P)^2 * \delta_*Q_1 \\
&\quad + (d-1) * \delta_*P * ((\delta_*Q_1)^2 - \delta_*Q_2) \\
&\quad - ((\delta_*Q_1)^3 - 2 * \delta_*Q_1 * \delta_*Q_2 + \delta_*Q_3). \\
\delta_*Ch_{11} &= \binom{d+1}{2}^2 * (\delta_*P)^2 - 2 * (d+1) * \delta_*P * \delta_*Q_1 + (\delta_*Q_1)^2.
\end{aligned}\right\} \tag{5.3.60}$$

关于代数簇的一些态射

考察 $\mathbf{K}$ 上 $P_{\mathbf{K}}^n$ 中维数为 d 的不可约代数簇 V. 令 Ξ 为 V 的母点, T_Ξ 为 V 在 Ξ 的切空间, 这是 $P_{\mathbf{K}}^n$ 中过点 Ξ 的维数为 d 的线性子空间. 对 (Ξ, T_Ξ) 是 $\mathrm{GR}(n;0,d)$ 中的一个点, 该点确定了 $\mathrm{GR}(n;0,d)$ 的一个以 (Ξ, T_Ξ) 为母点不可约子簇 $\hat{V}$:

$$\hat{V} = \mathrm{Spec}_{\mathbf{K}}\ (\Xi, T_\Xi) \subset \mathrm{GR}(n;0,d). \tag{5.3.61}$$

定义 5.3.23　Inverse tangential 态射

$$\tau_*\colon\ \mathrm{Alg}_*(\hat{V}) \longrightarrow \mathrm{Alg}_*(V) \tag{5.3.62}$$

定义为由

$$\tau\colon\ (X,T) \longrightarrow X \tag{5.3.63}$$

诱导的同态, 其中 $X \in V$, $(X,T) \in \hat{V}$.

对于余维数 $r \le d$ 的任意 Ehresmann 类 E, E 与 $\hat{V}$ 的相交是 $\hat{V}$ 的余维数为 r 的有定义的代数等价类.

定义 5.3.24　相交同态

$$\nu_*\colon\ \mathrm{Alg}_{D-r}(\mathrm{GR}(n;0,d)) \longrightarrow \mathrm{Alg}_{d-r}(\hat{V})\quad (0 \le r \le d) \tag{5.3.64}$$

定义为与非奇异簇 $\mathrm{GR}(n;0,d)$ 中的 $\hat{V}$ 的相交诱导的态射.

不可约簇的陈类与陈数

定义 5.3.25　对于任意如同 (5.3.49) 中维数 $r \le d$ 的 Ehresmann 类 E, 簇 V 的具有 Ehresmann符号 E 的 Ehresmann类$E(V)$ 定义为类

$$E(V) = \tau_*\nu_*\delta_*E \in \mathrm{Alg}_*(V). \tag{5.3.65}$$

定义 5.3.26　对于任意如同 (5.3.59) 中相对于分划 $\pi(p \le d)$ 的陈类 Ch_π, 簇 V 的相对于分划 π 的陈类 $Ch_\pi(V)$ 定义为类

$$Ch_\pi(V) = \tau_*\nu_*\delta_*Ch_\pi \in \mathrm{Alg}_p(V). \tag{5.3.66}$$

定义 5.3.27　对于任一代数等价类 $c \in \mathrm{Alg}_d(\mathrm{GR}(n;0,d))$, 簇 V 的陈数或陈特征标 $c(V)$ 定义为元素

$$c(V) = \tau_*\nu_*\delta_*c \in \mathrm{Alg}_0(V), \tag{5.3.67}$$

这里 $\mathrm{Alg}_0(V)$ 等同于 $\mathbf{Z}$.

记号 5.3.28 对于 d 的一个分划 π, 对应于类 $Ch_\pi \in \mathrm{Alg}_*(\mathrm{GR}(n;0,d))$ 的陈数 $:= Ch_\pi(V)$.

简单情形的例子

令 V_2 为 $P_{\mathbf{K}}^n(n \geq 3)$ 中的不可约代数曲面，则有相应于 V_2 的一些经典数值不变量.

定义 5.3.29 阶 $\mu_0(V_2) :=P_{\mathbf{K}}^n$ 中一个维数为 $n-2$ 的线性子空间与 V_2 相交的点的个数，或者等价地说， V_2 与 $P_{\mathbf{K}}^n$ 中的一个一般超曲面相交得到的相交曲线的次数.

秩 $\mu_1(V_2) := V_2$ 与 $P_{\mathbf{K}}^n$ 中的一个一般超曲面相交得到的相交曲线的秩.

类 $\mu_2(V_2) := V_2$ 与 $P_{\mathbf{K}}^n$ 中的一个一般超平面相交得到的相交曲线的类.

型 $\nu_2(V_2) := V_2$ 的切平面与 $P_{\mathbf{K}}^n$ 中的一个维数为 $n-4$ 的线性子空间相交的简单点的个数.

注意型仅仅被定义在 $n \geq 4$ 的情形.

定理 5.3.30 对于 $P_{\mathbf{K}}^n$ 中的不可约代数曲面，我们有

$$\begin{aligned}
\mu_0(V_2) &= \begin{bmatrix} 2 & & \\ 0 & 1 & 2 \end{bmatrix}(V_2),\\
\mu_1(V_2) &= \begin{bmatrix} 1 & & \\ 0 & 1 & 3 \end{bmatrix}(V_2),\\
\mu_2(V_2) &= \begin{bmatrix} 0 & & \\ 0 & 2 & 3 \end{bmatrix}(V_2),\\
\nu_2(V_2) &= \begin{bmatrix} 0 & & \\ 0 & 1 & 4 \end{bmatrix}(V_2).
\end{aligned} \tag{5.3.68}$$

证明 直接比较相应的定义即可. □

广义 Miyaoka-Yau 不等式

对于具有任意奇性的代数簇，定义 5.3.25, 5.3.26 为我们提供了把陈类和陈数的研究化为相交的研究的一般方法. 因为Grassmannians中的相交由(5.3.54)~(5.3.56) 显式地给出，所以研究最终简化为简单的计算. 并且，对于基域是复数域的情形，在像 Grassmannian 那样的非奇异簇中具有互补维数的两个代数子簇的相交数总是正的. 于是，这将导致借助于计算来研究陈数的正性. 作为上述可计算性原理和方法的一个具体的应用，下面我们考虑最简单情形.

Miyaoka 与 Yau (参见 [Miy1], [Yau1,2]) 已经证明, 3 维复射影空间中没有奇性的复代数曲面的陈数之间存在一些不平常的不等式:

$$3*ch_2(V_2) \geq ch_{11}(V_2). \tag{5.3.69}$$

根据上面的理论, 我们将证明该不等式对 $P_{\mathbf{C}}^3$ 中具有任意奇性的不可约代数超曲面都成立. 从上面的理论知道这是显然成立的.

定理 5.3.31 对于 $P_{\mathbf{C}}^3$ 中具有任意奇性的不可约复代数曲面 V_2, Miyaoka-Yau 不等式 (5.3.69) 成立.

证明 由 (5.3.60) 我们有

$$\begin{aligned} ch_2(V_2) &= [\delta_*(3*(\delta_*\ P)^2-2*\delta_*P*\delta_*Q_1+(\delta_*Q_1)^2-\delta_*Q_2)](V_2).\\ ch_{11}(V_2) &= [\delta_*(9*(\delta_*P)^2-6*\delta_*P*\delta_*Q_1+(\delta_*Q_1)^2)](V_2). \end{aligned} \tag{5.3.70}$$

从而有

$$3*ch_2(V_2)-ch_{11}(V_2) = [2*\delta_*(\delta_*Q_1)^2-3*Q_2](V_2). \tag{5.3.71}$$

由相交公式 (5.3.54)~(5.3.56) 可得, 上面最后等式的右边等于

$$2*\begin{bmatrix} 0 & & \\ 0 & 2 & 3 \end{bmatrix}(V_2)-\begin{bmatrix} 0 & & \\ 0 & 1 & 4 \end{bmatrix}(V_2). \tag{5.3.72}$$

在 $P_{\mathbf{C}}^3$ 中, 上面最后表达式中的第二项不存在, 而由定义知第一项是非负整数. 因此由 (5.3.71) 我们得到不等式 (5.3.69). 定理得证. □

用同样的方法, 我们有下面的

定理 5.3.32 对于 $P_{\mathbf{C}}^4$ 中 3 维不可约复超曲面 V_3, 我们有关于陈数的不等式

$$4*ch_{12}(V_3)-8*ch_3(V_3)-ch_{111}(V_3) \geq 0. \tag{5.3.73}$$

证明 如同定理 5.3.31 中的证明, 通过直接计算得

$$4*ch_{12}(V_3)-8*ch_3(V_3)-ch_{111}(V_3) = 5*\delta_*(\delta_*Q_1)^3(V_3). \tag{5.3.74}$$

由定义知, $\delta_*(\delta_*Q_1)^3(V_3)$ 是非负整数, 故我们从 (5.3.74) 即得 (5.3.73). □

注释 5.3.33 有例子表明 Miyaoka-Yau 不等式 (5.3.69) 对 $P_{\mathbf{C}}^4$ 中的不可约代数曲面不再成立, 可参见 [S-R], p.221.

注释 5.3.34 早在 1965 年前，对于具有任意奇性的代数簇的陈类与陈数由本文作者在计算方法中首先引入，参见 [WWT35,36]. 此后研究被中断且推迟到 1985 年 6 月才重新开始，见 [WWT37]. 这些概念也被不同的作者用各种不同的方法引进过，著名的有 MacPherson, 参见 [MP]. 在高维射影空间中没有奇性的不可约代数超曲面的陈数之间可能存在的不等式由 Tai 第一次给出，参见 [Tai]. 石赫用上面的方法研究了具有任意奇性的超曲面，参见 [SH1,2].

注释 5.3.35 有不同的作者通过不同的途径对具有任意奇性的代数簇引入了陈类和陈数的概念，其中比较著名的为 MacPherson 所引入，参见 [MP]. 然而，与这里给出的方法相比，他们的方法都不是可计算的. 刘先仿对 Nash, Mather, MacPherson 以及作者所引入的各种不同的定义作了比较，参见他的文章 [LXF] 及本书 §8.5.

§5.4 拟代数簇的投影定理

几何点集的参数化

记号 5.4.1 $\mathbf{K}, X = (x_1, \cdots, x_n)$, 等等，如前所述.

$T = (t_1, \cdots, t_p) :=$ 独立参数集合.

$A^p_{\mathbf{K}}(T) :=$ 在 $\mathbf{K}$ 上的仿射空间，坐标为 T.

$A^{n+p}_{\mathbf{K}}(X, T) := A^n_{\mathbf{K}}(X) \times A^p_{\mathbf{K}}(T)$.

定义 5.4.2 一个几何点集 $S \subset A^n_{\mathbf{K}}(X)$ 关于 *参数T* 被 *参数化* 是指存在有理函数 $g_i \in \mathbf{K}(T)$ 或多项式 $g_i \in \mathbf{K}[T]$, 其中 $i = 1, \cdots, n$, 使得对每一个在 S 中的点 $X^0 = (x^0_1, \cdots, x^0_n)$, 方程组

$$x_i = g_i(t_1, \cdots, t_p) \quad (i = 1, \cdots, n) \tag{5.4.75}$$

可解，即对 $\mathbf{K}$ 的某一扩域存在 $t_i = t^0_i$, 使得 $g_i(t^0_1, \cdots, t^0_p) = x^0_i$ $(i = 1, \cdots, n)$ 成立.

例 5.4.3 文献中通常说在空间 $A^2_{\mathbf{K}}(x_1, x_2)$ 上的一个圆 $C : x_1^2 + x_2^2 = 1$ 通过如下形式的 $\mathbf{K}(x_1, x_2)$ 中的有理函数用 1 个参数 t 被参数化:

$$x_1 = \frac{2 * t}{1 + t^2}, \ x_2 = \frac{1 - t^2}{1 + t^2}. \tag{5.4.76}$$

然而，这不完全正确，因为对圆 C 上的点 $X^0 = (x^0_1, x^0_2) = (0, -1)$, 方程 (5.4.76) 对 t 根本就无解. 这说明只有点集 $C \setminus \{(0, -1)\}$, 但不是整个圆 C 上的所有

点，通过 (5.4.76) 关于 t 参数化. 因而圆 C 的参数化方程 (5.4.76) 仅含有一个例外 的点，如 $X^0 = (0, -1)$.

注释 5.4.4 如果我们在定义 5.4.2 中的参数方程中不把想法限制在有理函数或多项式，那么，圆 C 可以用通常的三角函数来参数化：

$$x_1 = \sin\ t,\ x_2 = \cos\ t, \tag{5.4.77}$$

而不出现例外的点.

例 5.4.5 椭圆曲线

$$x_2^2 = 4 * x_1^3 - g_2 * x - g_3 \tag{5.4.78}$$

在复数空间中 $A^2_{\mathbf{C}}(x_1, x_2)$ 有关于 t 的参数化，它利用 Weierstrass 椭圆函数 $\mathcal{P}$ 和它们的导数 $\mathcal{P}'$, 得到

$$x_1 = \mathcal{P}(t),\ x_2 = \mathcal{P}'(t). \tag{5.4.79}$$

注意到现代代数几何证明甚至允许存在一些例外的点, (5.4.78) 仍不可能通过有理函数或多项式来参数化.

<u>参数化点集的隐式化</u>

定义 5.4.6 一个通过 (5.4.75) 由 $t_1, \cdots, t_p$ 参数化的几何点集 $S \subset A^n_{\mathbf{K}}(X)$ 的 *隐式化* 是指一个多项式集合 $PS \subset \mathbf{K}[X]$, 使得 S 和 Zero(PS) 相同，或

$$S = \text{Zero}(PS) \setminus S', \tag{5.4.80}$$

其中 S' 在某种待确切说明的意义上是 S 的可 *忽略* 的部分.

例 5.4.7 通过关于 t_1, t_2 的参数方程

$$x_1 = t_1 * t_2,\ x_2 = t_1 * t_2^2,\ x_3 = t_1^2 \tag{5.4.81}$$

给出一个几何点集 $S \subset A^3_{\mathbf{K}}(x_1, x_2, x_3)$. 首先我们证明 S 不是一个代数簇. 实际上，对独立变量 u 和 v, 对应于 $t_1 = u^2$, $t_2 = \frac{v}{u}$ 的点 $\Xi = (u * v, v^2, u^4)$ 在 S 中. 对任何值 $a \neq 0$, 点 $A = (0, a, 0)$ 显然是 Ξ 在 $\mathbf{K}$ 上的特定化，然而不存在任何值 t_1, t_2 能给出点 A. 这证明 S 不是一个代数簇，否则, $\Xi \in S$ 会推出 $A \in S$.

可以证明

$$S = \text{Zero}(x_2^2 * x_3 - x_1^4\ /\ x_1 * x_2) + \text{Zero}(x_1, x_2). \tag{5.4.82}$$

由它可得

$$S = \mathrm{Zero}(x_2^2 * x_3 - x_1^4) \setminus S',$$

其中 (5.4.83)

$$S' = \mathrm{Zero}(x_1, x_3 \mathbin{/} x_2).$$

对于 $\mathbf{K} = \mathbf{C}$, 点集 S 在实数空间 $A_{\mathbf{R}}^3(x_1, x_2, x_3)$ 的部分可以视为由在 x_3 为正常数的平面中向 x_2 轴和整个 x_3 轴收缩的抛物线

$$x_1^2 = \pm x_2 * \sqrt{x_3}$$

组成. 注意到由点 $(0, a, 0)$(其中 $a \neq 0$) 组成的去掉原点的 x_2 轴, 都不在点集 S 上.

隐式问题和几何轨迹问题

我们知道给出一个几何对象的参数化甚至用超越函数, 也只能在极少数情形可能做到. 由于这缘故, 我们在此不考虑这个问题. 另一方面, 我们将考虑已由下面形式参数化的几何对象的隐式化问题.

隐式化问题 Imp. 通过方程 (5.4.75) 给出一个参数化了的几何对象 S, 来决定一个多项式集合 $PS \subset \mathbf{K}[X]$, 使得 $\mathrm{Zero}(PS)$ 和 S 尽可能一样或 S 和 $\mathrm{Zero}(PS)$ 只差一个如 (5.4.80) 所示的可 *忽略* 的部分 S'.

注释 5.4.8 在文献中通常将方程 $PS = 0$ 称为给定几何对象 S 的 *隐式方程*, 如果它存在. 这个术语不完全准确, 因为例 5.4.5 中的 (5.4.83) 提到 S' 的部分是很难准确表述的. 由于这个原因我们将在本书中尽量避免使用这个术语.

一个和隐式化问题相关的重要的问题是下面的问题 L:

几何轨迹问题 L. 在 $A_{\mathbf{K}}^n(X)$ 中的一个动点 P 被几何约束在如下形式:

$$h_i(X, T) = 0,\ i = 1, \cdots, r, \tag{5.4.84}$$

其中 $h_i \in \mathbf{K}[X, T]$. 要尽可能的以方程 $PS = 0$ 的形式决定点 P 的几何轨迹, 其中 $PS \subset \mathbf{K}[X]$.

注释 5.4.9 作为一个特例, 问题 L 包括问题 Imp, 因为 (5.4.75) 可以转变为 (5.4.84) 的形式. 因此对问题 L, $\mathbf{K}[X]$ 中的多项式方程组的形式的解通常得不出来.

拟代数簇

由例 5.4.5 的 (5.4.82) 和 (5.4.83) 可以看出, 以形式 $\mathrm{Zero}(PS)(PS \subset \mathbf{K}[X])$ 来解决问题 Imp 或 L, 甚至是在很简单的情形下也是不可能的. 然而, 从 (5.4.82)

可以看出，如果我们采用形式 Zero(PS/G), 其中 $G \in \mathbf{K}[X]$, 就有可能解决问题. 因此，我们介绍下面的定义.

定义 5.4.10 在仿射空间 $A_{\mathbf{K}}^n(X)$ 里的一个 *拟代数簇* Q 是指一个点集 Q,

$$Q = \bigcup_i \text{Zero}(PS_i \ / \ G_i), \tag{5.4.85}$$

其中 $PS_i(i=1,\cdots,s)$ 是 $\mathbf{K}[X]$ 中的多项式集合, $G_i(i=1,\cdots,s)$ 是 $\mathbf{K}[X]$ 中的非零多项式.

注释 5.4.11 拟代数簇在 $A_{\mathbf{K}}^{n+p}(X,T)$ 上或其他仿射空间中同样定义.

投影问题和投影定理

我们从另外的角度来考虑问题 Imp 和 L, 提出下面的记号和定义.

记号 5.4.12 $A_{\mathbf{K}}^N(Z) := \mathbf{K}$ 上 N 维仿射空间，坐标为 $Z=(z_1,\cdots,z_N)$.

$K := \{1,\cdots,N\}$ 的子集 $\{k_1,\cdots,k_q\}$, k 的坐标升序排列.

$J :=$ 与 K 互补的 $\{1,\cdots,N\}$ 的子集.

$A_{\mathbf{K}}^q(Z') := A_{\mathbf{K}}^N(Z)$ 的仿射子空间，由方程 $z_j=0(j\in J)$ 定义，坐标为 $Z'=(z_{k_1},\cdots,z_{k_q})$.

定义 5.4.13 如记号 5.4.12 所述，仿射空间 $\mathbf{A}_1 = A_{\mathbf{K}}^N(Z)$ 到子空间 $\mathbf{A}_2 = A_{\mathbf{K}}^q(Z')$ 的 *投影* 定义为 $\mathbf{A}_1$ 到 $\mathbf{A}_2$ 的映射 π, 由 $\pi(Z)=Z'$ 定义.

记号 5.4.14 对 $\mathbf{A}_1 = A_{\mathbf{K}}^{n+p}(X,T)$ 和 $\mathbf{A}_2 = A_{\mathbf{K}}^n(X)$ 如定义 5.4.13 所述的投影记为 $\pi_{n+p,n}$.

投影问题 P. 给定仿射空间 $\mathbf{A}_1 = A_{\mathbf{K}}^{n+p}(X,T)$ 中的代数簇或拟代数簇 U, 要研究 U 在映射 $\pi_{n+p,n}$ 下的像是不是一个代数簇或拟代数簇.

例 5.4.3, 5.4.5 说明，如果我们把 U 和它的像只限制在代数簇，问题 P 是不成立的. 另一方面，如果 U 和它的像是 *拟代数簇* 的话，答案是肯定的，这由下面的定理给出.

定理 5.4.15 (投影定理) 仿射空间 $\mathbf{A}_1 = A_{\mathbf{K}}^{n+p}(X,T)$ 中拟代数簇在仿射空间 $\mathbf{A}_1$ 到仿射空间 $\mathbf{A}_2 = A_{\mathbf{K}}^n(X)$ 的投影 $\pi_{n+p,n}$ 下的像仍然是一个拟代数簇，这个像可以由算法显式确定.

我们将把定理的证明推迟到后面的章节中.

注释 5.4.16 显然投影问题 P 可以被认为是几何约束轨迹问题 L 的另一种形式.

注释 5.4.17 拟代数簇的概念在通常的代数几何专著中已经出现过，但是这一概念很少有文献研究过. 然而从第 3 章的良序原理和零点分解定理中

看到拟代数簇在我们的理论中扮演着基本的角色.

例 5.4.18 考虑代数簇 $V = \text{Zero}(x_1 * t - 1) \subset A^2_{\mathbf{K}}[x_1, t]$. V 到子空间 $A^1_{\mathbf{K}}(x_1)$ 的投影是一个拟代数簇 $\text{Zero}(\emptyset \ / \ x_1)$, 它不是 $A^1_{\mathbf{K}}(x_1)$ 里的代数簇.

注释 5.4.19 由第 3.2 节中的公式 (3.2.9) 看到代数簇在集合的并和交的运算下显然是封闭的, 前面的例 5.4.18(或例 5.4.3, 5.4.5) 表明代数簇在投影运算下不是封闭的. 另一方面, 由投影定理所示, 拟代数簇不但在集合的并和交的运算下是封闭的, 而且在投影的运算下也封闭.

<u>关于拟代数簇的一些引理</u>

显然, 一般的投影定理可以运用 $p = 1$ 的特殊情形得到, 或从 $A^{n+1}_{\mathbf{K}}(X, t)$ 到子空间 $A^n_{\mathbf{K}}(X)$ 的投影的情形得到. 因此, 我们将更详细研究带有特殊坐标 t 的 $A^{n+1}_{\mathbf{K}}(X, t)$ 中的拟代数簇的投影. 下面我们先安排变量的序:

$$x_1 \prec \cdots \prec x_n \prec t. \tag{5.4.86}$$

定义 5.4.20 在仿射空间 $A^{n+1}_{\mathbf{K}}(X, t)$ 中 *类型 d 的 简单拟代数簇* 是指有如下形式的拟代数簇 Z:

$$Z = \text{Zero}(XS, F \ / \ G * H), \tag{5.4.87}$$

其中

$$XS \subset \mathbf{K}[X], \ F, G \in \mathbf{K}[X, t], \ H \in \mathbf{K}[X],$$

并且 $deg_t \ F = d$, 其中 $d > 0$, 而对于 $d = 0$, 则 F 略去.

下面的引理将把对任何在 $A^{n+1}_{\mathbf{K}}(X, t)$ 中的拟代数簇的研究简化到对简单拟代数簇的研究.

引理 5.4.21 在 $A^{n+1}_{\mathbf{K}}(X, t)$ 中任何拟代数簇

$$\text{Zero}(PS \ / \ G * H), \tag{5.4.88}$$

其中 $PS \subset \mathbf{K}[X, t], G \in \mathbf{K}[X, t]$, 而 $H \in \mathbf{K}[X]$, 是由每一形如 (5.4.87) 的简单拟代数簇的并组成, 其中, 如果 F 出现, 则 H 可以被 F 关于变量序 (5.4.86) 的初式整除.

证明 通过第 3.4 节的零点分解定理, 我们有升列 AS_k 的集合 (其中初式积为 IP_k) 和如下形式的分解:

$$\text{Zero}(PS) = \bigcup_k \text{Zero}(AS_k \ / \ IP_k).$$

根据变量序 (5.4.86), 每一个 AS_k 有如下形式:

$$AS_k = XS_k + \{F_k\},$$

其中 $XS_k \subset \mathbf{K}[X]$ 而且 $F_k \in \mathbf{K}[X,t]$, $deg_t\ F_k = d_k > 0$, 如果 F_k 出现. 另一方面, 如果这样的 F_k 不存在, 这时令 $d_k = 0$. 于是, 我们有

$$\mathrm{Zero}(PS\ /\ G * H) = \bigcup\nolimits_k\ \mathrm{Zero}(XS_k, F_k\ /\ G * H_k),$$
$$H_k = H * IP_k \in \mathbf{K}[X].$$

不论 F_k 是否存在, 显然初式积 IP_k 在 $\mathbf{K}[X]$ 中. 由此推出在最后一个并中的成员是具有初式 IP_k 类型为 d_k 的简单拟代数簇. 因而也有 F_k 的初式作为因子, 如果 F_k 出现. 引理得证. □

现在让我们来考虑 (5.4.87) 中的两种简单拟代数簇的特殊的情形, 它们或者缺少 F, 或者缺少 G.

引理 5.4.22 在 $A_{\mathbf{K}}^{n+1}(X,t)$ 中的如 (5.4.87) 中类型为 0(F 不存在) 的简单拟代数簇

$$Z_0 = \mathrm{Zero}(XS\ /\ G * H).$$

它的投影 $\pi_{n+1,n}(Z_0)$ 是在 $A_{\mathbf{K}}^n(X)$ 中的拟代数簇.

证明 如果 G 不存在, 那没什么可以证明的了. 否则让我们把 G 写成标准形式

$$G = B_0 * t^e + \cdots + B_e,\ e = deg_t\ G > 0,\ B_i \in \mathbf{K}[X].$$

对 $i = 0, 1, \cdots, e$, 设

$$XS_i = XS + \{B_0, \cdots, B_{i-1}\},$$

这里约定 $XS_0 = XS$. 易知

$$\pi_{n+1,n}(Z_0) = \mathrm{Zero}(XS\ /\ B_e * H) + \bigcup_i\ \mathrm{Zero}(XS_i\ /\ B_i * H), \tag{5.4.89}$$

并遍历 $i = 0, \cdots, e$. 实际上, 令 (X', t') 是 Z_0 上的任意点, 且 $\pi_{n+1,n}(X', t') = X'$.

如果 $t' = 0$, 那么 $G(X', t') = B_e(X') \neq 0$, 因此 $X' \in \mathrm{Zero}(XS/B_e * H)$.

故可假设 $t' \neq 0$. 于是 $G(X', t') \neq 0$, 因此或者 $B_0(X') \neq 0$, 或者对某一 $i = 1, \cdots, e$, 我们有 $B_0(X') = 0, \cdots, B_{i-1}(X') = 0$, 但 $B_i(X') \neq 0$. 前一种情形 $X' \in \mathrm{Zero}(XS/B_0 * H)$, 而后一种情形 $X' \in \mathrm{Zero}(XS_i\ /\ B_i * H)$. 因此 $\pi_{n+1,n}(Z_0)$ 包含于恒等式 (5.4.89) 右边. 反之, 考虑 (5.4.89) 右边的任意点 X'.

如果 $X' \in \text{Zero}(XS/B_e * H)$, 那么 $G(X',0) = B_e(X') \neq 0$, 因此 $(X',0) \in Z_0$, 由此 $X' = \pi_{n+1,n}(X',0) \in \pi_{n+1,n}(Z_0)$. 如果 $X' \in \text{Zero}(XS/B_0 * H)$, 那么 $B_0(X') \neq 0$. 于是我们可以任取 t', 使得 $G(X',t') \neq 0$, 因此 $(X',t') \in Z_0$.

如果对某一 $i = 1, \cdots, e$, 我们有 $X' \in \text{Zero}(XS_i \ / \ B_i * H)$, 那么 $B_0(X') = 0, \cdots, B_{i-1}(X') = 0$, 而 $B_i(X') \neq 0$. 在这种情况下, 我们有 $G(X',t) = B_i(X') * t^{e-i} + \cdots + B_e(X')$, 其中首项系数 $B_i(X') \neq 0$, 则我们可以取 t', 使得 $G(X',t') \neq 0$, 于是又有 $(X',t') \in Z_0, X' \in \pi_{n+1,n}(Z_0)$. 由此, (5.4.89) 的右边的也包含在 $\pi_{n+1,n}(Z_0)$ 中. 这就证明了恒等式 (4.15). 又因为 (4.15) 的右边的每一成员都是 $A^n_{\mathbf{K}}(X)$ 中的拟代数簇, 引理得证. □

引理 5.4.23 对于在 $A^{n+1}_{\mathbf{K}}(X,t)$ 中如 (5.4.87), G 不出现的简单拟代数簇

$$Z' = \text{Zero}(XS, F \ / \ H),$$

那么 Z' 在 $\pi_{n+1,n}$ 下的投影是 $A^n_{\mathbf{K}}(X)$ 中的拟代数簇.

证明 把 $F \in \mathbf{K}[X,t]$ 写成标准形式

$$F = A_0 * t^d + \cdots + A_d, \ A_i \in \mathbf{K}[X], \ d = Deg_t \ F > 0.$$

对 $i = 0, 1, \cdots, d, d+1$, 令

$$F_i = A_i * t^{d-i} + \cdots + A_d,$$

$$XS_i = XS + \{A_0, \cdots, A_{i-1}\},$$

约定 $XS_0 = XS$, 则显然有

$$Z' = \bigcup_i \text{Zero}(XS_i, F_i \ / \ H * A_i),$$

并遍历 $i = 0, \cdots, d+1$. 注意到在并中对应于 $i = d$ 的成员是空的, 对应于 $i = d+1$ 的成员已经是 $A^n_{\mathbf{K}}(X)$ 中的拟代数簇. 如同前面引理的证明容易看出, 对每一个 $i \leq d-1$,

$$\pi_{n+1,n} \ \text{Zero}(XS_i, F_i \ / \ H * A_i) = \text{Zero}(XS_i \ / \ H * A_i).$$

因为以上的每一个是 $A^n_{\mathbf{K}}(X)$ 中的拟代数簇, 所以 $\pi_{n+1,n}(Z')$ 也是. 引理得证. □

<u>投射定理的证明</u>

我们现在证明 $p = 1$ 或 $\pi_{n+1,n}$ 的情形的投射定理.

证明　根据引理 5.4.21~5.4.23, 我们只要考虑如 (5.4.87) 形式的拟代数簇 Z, 它满足下面的条件:

(a) $Deg_t\ F = d > 0$.

(b) $Deg_t\ G > 0$.

(c) H 可以被 $F(\in \mathbf{K}[X,t])$ 中的初式 $I \in \mathbf{K}(X)$ 整除.

我们先求出 G^d 关于 F 的余式 $R \in \mathbf{K}[X,t]$, 因此对某一非负整数 s 我们有

$$I^s * G^d = Q * F + R,\ Deg_t\ R < d. \tag{5.4.90}$$

令

$$Z' = \mathrm{Zero}(XS\ /\ G * H * R), \tag{5.4.91}$$

那么对 (5.4.87) 中的任意零点 $(X',t') \in Z$, 我们有 $G(X',t') \neq 0$ 和 $H(X') \neq 0$. 因此根据 (c) 我们也有 $I(X') \neq 0$. 另一方面 $F(X',t') = 0$. 因此根据 (5.4.90) 有 $R(X',t') \neq 0$, 所以 (X',t') 属于 Z'. 因此 Z 包含在 Z' 中, 所以

$$\pi_{n+1,n}(Z) \subset \pi_{n+1,n}(Z'). \tag{5.4.92}$$

要看反方向的包含关系, 先让我们考虑 R 恒为 0 的情形, 则 Z' 是空的, 因此我们有 $Z' \subset Z$, 于是

$$\pi_{n+1,n}(Z') \subset \pi_{n+1,n}(Z). \tag{5.4.93}$$

因此我们考虑 R 不恒为 0 的情形. 令 X' 是 $\pi_{n+1,n}(Z')$ 中的任一个零点, 如果它存在. 那么就存在某个 t', 使得 (X',t') 属于 Z'. 于是特别地我们有

$$\left.\begin{array}{l} R(X',t') \neq 0, \\ G(X',t') \neq 0, \\ H(X') \neq 0. \end{array}\right\} \tag{5.4.94}$$

根据 (c), 我们又有

$$I(X') \neq 0.$$

由此 $F(X',t)$ 中的 t 的次数和 $F(X,t)$ 的一样为 $d > 0$. 如果现在 $F(X',t)$ 的任何零点 t'' 也是 $G(X',t)$ 的零点, 那么 $F(X',t)$ 是 $G(X',t)^d$ 的一个因子. 根据 (5.4.90), 则 $F(X',t)$ 也是 $R(X',t)$ 的因子. 因为只有当 $R(X',t)$ 恒为 0 时, $R(X',t)$ 的 t 的次数可能比 $F(X',t)$ 的次数 d 低, 但这和 (5.4.94) 的第一式矛

盾. 因此至少有 $F(X',t)$ 的一个零点 t'' 不是 $G(X',t)$ 的零点. 于是 (X',t'') 属于 Z 因此 $X' = \pi_{n+1,n}(X',t'')$ 属于 $\pi_{n+1,n}(Z)$. 这证明了 (5.4.93), 结合 (5.4.92), 我们有

$$\pi_{n+1,n}(Z) = \pi_{n+1,n}(Z'). \tag{5.4.95}$$

根据引理 5.4.22, $\pi_{n+1,n}(Z')$ 是 $A^n_{\mathbf{K}}(X)$ 中的拟代数簇. 因此根据 (5.4.95), $\pi_{n+1,n}(Z)$ 也是 $A^n_{\mathbf{K}}(X)$ 中的拟代数簇. 因为引理 5.4.21~5.4.23 的证明中的分解是算法化的, 所以投射 $\pi_{n+1,n}(Z)$ 作为拟代数簇的实现也是算法化的. 这就完全证明了 $p=1$ 的情形的投射定理. 因而也证明了一般情形的投射定理. □

注释 5.4.24 投影定理至少在 $\mathbf{K}$ 是实数域 $\mathbf{R}$ 时是广为所知的, 那时术语拟代数簇用 *半代数* 集合来代替, 参考如 [B-C-R]. 作者不知道一般情形下的投影定理是否已知. 无论如何, 与现代代数几何中流行的 *存在性* 证明不同, 我们对定理的证明是 *构造性* 的. 因而我们的证明不但说明了拟代数簇的投影还是拟代数簇, 而且给出了投影后的拟代数簇的详细的形式.

§5.5 实多项式的极值性

极值点和极值

记号 5.5.1 $X := (x_1,\cdots,x_n)$.

$O :=$ $\mathbf{R}^n(X)$ 中的开区域.

$D :=$ $\mathbf{R}^n(X)$中开或非开的区域.

$HS := \{h_1,\cdots,h_m\} \subset \mathbf{R}[X]$.

$N := \{1,\cdots,n\}; M := \{1,\cdots,m\}$.

$T :=$ m 元组集, $(i_1,\cdots,i_m)$, 其中 $i_k \in N$ 且 $1 \le i_1 < \cdots < i_m \le n$.

$X_t := (x_{i_1},\cdots,x_{i_m})$, 对于 $t = (i_1,\cdots,i_m) \in T$.

$f,g :=$ $\mathbf{R}^n(X)$中多项式.

定义 5.5.2 $X^0 \in \mathbf{R}^n(X)$ 是 f 在 D 中的 *极值点* 或 *极值零点*, 或 f 在限制条件 $HS=0$ 及 $g \neq 0$ 下于 D 中在 X^0 处取得其局部极值是指 $X^0 \in D\mathrm{Zero}_{\mathbf{R}}(HS/g)$, 且在 $\mathbf{R}^n(X)\backslash\mathrm{Zero}_{\mathbf{R}}(HS/g)$ 中存在 X^0 的邻域 V, 使得对 $V_D = V\bigcap D$, 或者有 $f(X') \ge f(X^0)$, 对于任意 $X' \in V_D\mathrm{Zero}_{\mathbf{R}}(HS/g)$; 或者有 $f(X') \le f(X^0)$, 对于 $X' \in V_D\mathrm{Zero}_{\mathbf{R}}(HS/g)$.

定义 5.5.3 实数 r 是 f 于限制条件 $HS=0$ 及 $g \neq 0$ 下在区域 D 中的 *极值* 是指实数 $r = f(X^0)$, 其中 X^0 是 f 在限制条件 $HS=0$ 及 $g \neq 0$ 下在区

域 D 中的某一极值点.

缩写 5.5.4 E- 点 := 极值点. E- 值 := 极值. E- 零点 := 极值零点.

记号 5.5.5 $EZero_R(f,g,D,HS) := f$ 在限制条件 $HS=0$ 及 $g\neq 0$ 下于区域 D 中的极值点集.

$\mathrm{EVal}_R(f,g,D,HS) := f$ 在限制条件 $HS=0$ 及 $g\neq 0$ 下于区域 D 中的极值之集.

$EZero_R(f,D,HS)$ 或 $EZero_R(f,g,D)$ 或 $EZero_R(f,D) := EZero_R(f,g,D,HS)$ 在无 g 或无 HS 或两者均无的情形.

$\mathrm{EVal}_R(f,D,HS)$ 或 $\mathrm{EVal}_R(f,g,D)$ 或 $\mathrm{EVal}_R(f,D) := \mathrm{EVal}_R(f,g,D,HS)$ 在无 g 或无 HS 或两者均无的情形.

注释 5.5.6 上述定义显然可扩展到 f,g,h_i 均是可微函数情形. 后面我们会看出把其限制在多项式的好处.

<u>极值点与极值确定的基本问题</u>

极值问题 E 或 $\mathbf{E}\{f,g,D,HS\}$. 对给定的 f,g,D,HS 确定 $EZero_{\mathbf{R}}\{f,g,D,HS\}$ 及 $\mathrm{EVal}_{\mathbf{R}}\{f,g,D,HS\}$.

例 5.5.7 令 $n=2$, $(x_1,x_2)=(x,y)$, $D=\mathbf{R}^2(x,y)$, $f=x^2+y^2$, 而 $HS=\{h_1\}$, $h_1=(x-1)^3-y^2$. 那么, $X^0=(1,0)$ 显然是 f 在限制条件 $HS=0$ 下的极值点, 相应极值 $r=1$. 如图 5.1 所示.

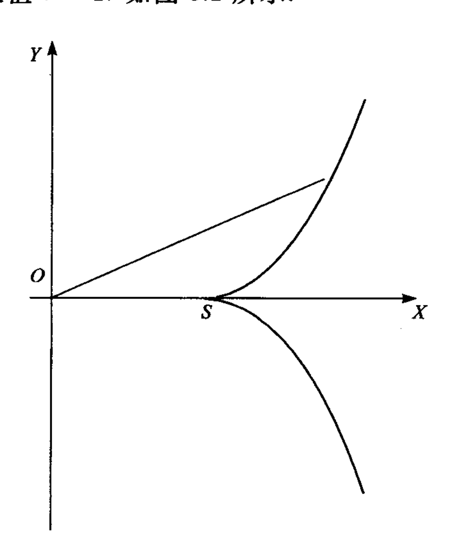


图 5.1 极值点与极值确定的基本问题

注释 5.5.8 从微积分学出现后，问题 **E** 就可以用微分方法给予成功的解决. 然而无论从理论或实际应用考虑，此问题远非一平凡的问题. 因为，即使对于开区间上的一元函数这种简单的情形，微积分学仅提供了充分或必要条件，而充要条件却从未给出. 另一方面，对于实际上极值点或极值的确定，微积分学常用的 Lagrange 乘子法总要导致方程求解. 而对于 f, g, h_i 是一般的可微函数的情形，并没有通用的方法来解此方程. 下面我们会看到，把函数限制在多项式情形是很合适的.

Lagrange 乘子法

下面我们将考虑对给定 f, g, D, HS 的问题 **E**, 其中 D 是 $\mathbf{R}^n(X)$ 中的开区域 O.

定义 5.5.9 关于 Lagrange 乘子 $\lambda_j (j \in M)$ 的 *Lagrange 多项式* 定义为

$$L = f + \sum_{j \in M} \lambda_j * h_j. \tag{5.5.96}$$

定义 5.5.10 *Lagrange 多项式集* 定义为

$$LS = \left\{ \frac{\partial L}{\partial x_i}, h_j | i \in N, j \in M \right\}. \tag{5.5.97}$$

定义 5.5.11 关于 $t = (i_1, \cdots, i_m) \in T$ 的 *Jacobi 行列式* 定义为

$$J_t = \frac{\partial(h_1, \cdots, h_m)}{\partial(x_{i_1}, \cdots, x_{i_m})} = \left| \frac{\partial h_j}{\partial x_{i_k}} \right|, \tag{5.5.98}$$

其中对于 m 元组 $t = (i_1, \cdots, i_m) \in T$, $\frac{\partial h_j}{\partial x_{i_k}}$ 是矩阵的第 j 行第 k 列元素.

定义 5.5.12 *Jacobi 多项式集* 是指多项式集

$$JS = \{J_t, h_j |\ t \in T, j \in M\}. \tag{5.5.99}$$

记号 5.5.13 $\Lambda = (\lambda_1, \cdots, \lambda_m) :=$ Lagrange 乘子集,

$$\widetilde{O} = O \times \mathbf{R}^m(\Lambda) \subset \mathbf{R}^{n+m}(X, \Lambda).$$

定义 5.5.14 对 $\Lambda = (\lambda_1, \cdots, \lambda_m)$, *Lagrange 映射* 定义为自然映射:

$$\text{LProj} : \mathbf{R}^{n+m}(X, \Lambda) \to \mathbf{R}^n(X), \text{ 其中LProj}(X, \Lambda) = X. \tag{5.5.100}$$

下述定理是一经典定理，例如可参见 [Cou], p.198.

定理 5.5.15 对于 $D = O$ 是开集的问题 **E**, 我们有

$$E\text{Zero}_{\mathbf{R}}\{f, g, O, HS\} \subset \text{LProj}\widetilde{O}\text{Zero}_{\mathbf{R}}(LS/g) + O\text{Zero}_{\mathbf{R}}(JS/g). \tag{5.5.101}$$

证明 假设

$$X^0=(x_1^0,\cdots,x_n^0)\in E\mathrm{Zero}_{\mathbf{R}}\{f,g,O,HS\}\backslash O\mathrm{Zero}_{\mathbf{R}}(JS/g), \tag{5.5.102}$$

我们只需证明

$$X^0\in \mathrm{LProj}\widetilde{O}\mathrm{Zero}_{\mathbf{R}}(LS/g). \tag{5.5.103}$$

由 (5.5.102) 可知，存在 T 中 m 元组 $t=(i_1,\cdots,i_m)$, 使得

$$\text{在}X^0\text{点}, J_t\neq 0. \tag{5.5.104}$$

改记 $x_{ik}=y_k$, 其余 x_i 改记为 $u_1,\cdots,u_d$, 其中 $d+m=n$. 那么对某置换 Perm, 我们有

$$\begin{aligned} y_k=x_{ik},\qquad k=1,\cdots,m,\qquad t=(i_1,\cdots,i_m)\in T,\\ X^0=(x_1^0,\cdots,x_n^0)=\mathrm{Perm}(u_1^0,\cdots,u_d^0,y_1^0,\cdots,y_r^0). \end{aligned} \tag{5.5.105}$$

由 (5.5.102) 存在点 $X^0\in O$ 且在 X^0 点 $g\neq 0$. 令 $U=(u_1,\cdots,u_d)$, 由隐函数定理知，存在 $\mathbf{R}^d(U)$ 中 $U^0=(u_1^0,\cdots,u_d^0)$ 点的邻域 $V(\subset O)$ 及 V 中一连续可微函数 $\phi_j(U)$, 使得对

$$y_j=\phi_j(u_1,\cdots,u_d),\qquad j\in M, \tag{5.5.106}$$

我们有

$$y_j^0=\phi_j(u_1^0,\cdots,u_d^0) \tag{5.5.107}$$

及

$$h_j(\mathrm{Perm}(u_1,\cdots,u_d,\phi_1,\cdots,\phi_m))=0\ \text{在}V\text{中}. \tag{5.5.108}$$

把 V 取得充分小使得在 V 上 $g\neq 0$. 对 (5.5.108) 微分可得

$$\frac{\partial h_j}{\partial u_k}+\sum_{l\in M}\left(\frac{\partial h_j}{\partial y_l}*\frac{\partial \phi_l}{\partial u_k}\right)=0\quad \text{在}V\text{中},\ j\in M,\quad k=1,\cdots,d. \tag{5.5.109}$$

现在作为 $u_1,\cdots,u_d$ 的函数,

$$f(\mathrm{Perm}(u_1,\cdots,u_d,\phi_1,\cdots,\phi_m)) \tag{5.5.110}$$

在没有更多限制方程的条件下，显然在 $U^0=(u_1^0,\cdots,u_d^0)\in V$ 点取得局部极值. 那么可知函数关于任一 u_k 的全导数在 U_0 点均是 0, 也即

$$\frac{\partial f}{\partial u_k}+\sum_{l\in M}\left(\frac{\partial f}{\partial y_l}*\frac{\partial \phi_l}{\partial u_k}\right)=0 \qquad \text{在}X^0\text{点}. \tag{5.5.111}$$

视 λ_j 为 X 的函数，现在对 (5.5.96) 微分可得

$$\left.\begin{aligned}\frac{\partial L}{\partial y_l}&=\frac{\partial f}{\partial y_l}+\sum_{j\in M}\lambda_j*\frac{\partial h_j}{\partial y_l}+\sum_{j\in M}\frac{\partial \lambda_j}{\partial y_l}*h_j, \quad l\in M\\ \frac{\partial L}{\partial u_k}&=\frac{\partial f}{\partial u_k}+\sum_{j\in M}\lambda_j*\frac{\partial h_j}{\partial u_k}+\sum_{j\in M}\frac{\partial \lambda_j}{\partial u_k}*h_j, \quad k=1,\cdots,d\end{aligned}\right\} \tag{5.5.112}$$

因为 $X^0\in O\text{Zero}_{\mathbf{R}}(HS/g)$, 于是在 X^0 点 $(5.5.112)_1$,$(5.5.112)_2$ 最后一和式均是 0. 另一方面，由 (5.5.104) 知，在 X_0 点 $(5.5.112)_1$ 中关于 λ_j 的系数矩阵的行列式 $J_t\neq 0$. 这样，我们可在 X^0 点解方程

$$\frac{\partial L}{\partial y_l}=0, \quad l\in M, \tag{5.5.113}$$

得到 $\Lambda=\Lambda^0=(\lambda_1^0,\cdots,\lambda_m^0)$. 由 $(5.5.112)_1$ 知

$$\frac{\partial L}{\partial y_l}=0 \quad \text{在}(X^0,\Lambda^0)\text{点}, \qquad l\in M. \tag{5.5.114}$$

对固定的 $k=1,\cdots,d$, 用 $\frac{\partial \phi_l}{\partial u_k}, l\in M$ 乘 (5.5.114) 并相加，那么由 (5.5.109), (5.5.111), $(5.5.112)_2$, 我们有

$$\frac{\partial L}{\partial u_k}=0 \qquad \text{在}(X^0,\Lambda^0)\text{点}. \tag{5.5.115}$$

从 (5.5.108), (5.5.114), (5.5.115) 我们可知 (X^0,Λ^0) 在 $\widetilde{O}\text{Zero}_{\mathbf{R}}(LS/g)$ 内，因此 X^0 在 $\text{LProj}\widetilde{O}\text{Zero}_{\mathbf{R}}(LS/g)$ 内. 这就证明了 (5.5.101). 从而证明了定理. □

注释 5.5.16 (5.5.101) 的右边包含 JS 的项不能被省去，事实上，从例 5.5.7 看出

$$L=x^2+y^2+\lambda_1*((x-1)^3-y^2)),$$
$$LS=\{2*x+3*\lambda_1*(x-1)^2, 2*y-2*\lambda_1*y, (x-1)^3-y^2\},$$
$$JS=\{3*(x-1)^2, -2*y, (x-1)^3-y^2\}.$$

我们看到

$$\text{Zero}_{\mathbf{R}}(LS)=\emptyset, \qquad \text{Zero}_{\mathbf{R}}(JS)=\{(1,0)\}.$$

因此，极值点 $X^0=(1,0)$ 在 $\text{Zero}_{\mathbf{R}}(JS)$ 中但不在 $\text{LProjZero}_{\mathbf{R}}(LS)$ 中.

注释 5.5.17 对于函数 f, g, h_i 是可微函数情形, 定理 5.5.15 仍是正确的. 其把寻找极值点的范围限制在求解方程 $LS = 0$ 及 $JS = 0$ 上. 目前对于一般情形, 解此方程是很困难的. 或许也正是此因, 如今 Lagrange 方法并不如以前得到广泛应用. 然而, 如我们把 f, g, h_i 限制在多项式情形, 方程 $LS = 0, JS = 0$ 成了多项式方程, 对此我们是可用我们的一般方法处理的. 这正是下面我们将要做的.

注释 5.5.18 对于 X^0 是极值点的判定, 定理 5.5.15 仅提供了一必要条件, 即对某些适当的 Lagrange 乘子值, 其应满足方程 $LS = 0$ 及 $JS = 0$. 因而即使我们能够求解这些方程, 一般也没有方法能判定这些解是否确实给出了极值. 但是如下所示, 对于 f, g, h_i 是多项式情形, 此困难是可被克服的.

HS 是升列的特殊情形

我们考虑 HS 是升列的特殊情形, 区域 $D = O$ 是开集. 利用某些如 (5.5.105) 所示的置换及 $U = (u_1, \cdots, u_d), Y_j = (y_1, \cdots, y_j), y_j = x_{i_j}, j \in M$, 我们可假设 $h_j \in HS$ 具有下述形式:

$$h_j = I_j * y_j^{d_j} + \text{关于}y_j\text{的更低项}, \qquad j \in M, \tag{5.5.116}$$

其中 y_j 的幂次的系数在 $\mathbf{R}[U, Y_{j-1}]$ 中.

引理 5.5.19 假设多项式集 HS 是以 ISP 为其初式隔离子积的升列, 那么我们有

$$O\text{Zero}_{\mathbf{R}}(JS/ISP) = \emptyset \tag{5.5.117}$$

以及

$$E\text{Zero}_{\mathbf{R}}\{f, ISP, O, HS\} \subset \text{LProj}\widetilde{O}\text{Zero}_{\mathbf{R}}(LS/ISP) \subset O\text{Zero}_{\mathbf{R}}(HS/ISP). \tag{5.5.118}$$

证明 在 Jacobi 多项式集中存在

$$J_t = \frac{\partial(h_1, \cdots, h_m)}{\partial(y_1, \cdots, y_m)}, \qquad t = (i_1, \cdots, i_m).$$

由 (5.5.116), 对 $j, k \in M$, 我们有

$$\frac{\partial h_j}{\partial y_k} = 0 \text{ 对} k > j, \qquad \frac{\partial h_j}{\partial y_j} = S_j, \tag{5.5.119}$$

其中 S_j 是 h_j 的隔离子. 由此可知

$$J_t = S_1 * S_2 * \cdots * S_m,$$

因此

$$OZero_{\mathbf{R}}(JS/ISP) = \emptyset.$$

这也就证明了 (5.5.117). 由定理 5.5.15 由此也有 (5.5.118) 成立. □

引理 5.5.20 令 HS 及 ISP 如引理 5.5.19 所示. 假设

$$f(X) = x_1. \tag{5.5.120}$$

令 Proj_1 是 $\mathbf{R}^{n+r}(X,\Lambda)$ 或 $\mathbf{R}^n(X)$ 到 $\mathbf{R}$ 的映射, 定义如下:

$$\left.\begin{array}{l}\mathrm{Proj}_1(X,\Lambda) = x_1 \\ \text{或} \\ \mathrm{Proj}_1(X) = x_1,\end{array}\right\} \tag{5.5.121}$$

那么存在一实有限集 (可能为空)

$$K\{x_1, ISP, O, HS\} \subset \mathrm{Proj}_1\widetilde{O}\mathrm{Zero}_{\mathbf{R}}(LS/ISP) \subset \mathbf{R}, \tag{5.5.122}$$

使得

$$\mathrm{EVal}_{\mathbf{R}}\{x_1, ISP, O, HS\} \subset K\{x_1, ISP, O, HS\} \subset \mathrm{Proj}_1 O\mathrm{Zero}_{\mathbf{R}}\{HS/ISP\}. \tag{5.5.123}$$

证明 变量 x 的选择仅可能是 u_1 或 y_1, 首先考虑 $x_1 = u_1$ 情形, 那么由 (5.5.120) 我们有

$$\frac{\partial f}{\partial y_1} = \frac{\partial f}{\partial y_2} = \cdots = \frac{\partial f}{\partial y_m} = 0, \quad \frac{\partial f}{\partial u_1} = 1. \tag{5.5.124}$$

考虑点

$$(X^0, \Lambda^0) \in \widetilde{O}\mathrm{Zero}(LS/ISP), \tag{5.5.125}$$

其中

$$X^0 = (x_1^0, \cdots, x_n^0), \quad \Lambda^0 = (\lambda_1^0, \cdots, \lambda_m^0).$$

对 $j \in M$ 我们有

$$\left.\begin{array}{l}\dfrac{\partial L}{\partial y_j} = 0 \quad \text{在}(X^0, \Lambda^0) \\ \text{及} \\ h_j = 0, S_j = \dfrac{\partial h_j}{\partial y_j} \neq 0 \text{ 在} X^0\end{array}\right\} \tag{5.5.126}$$

对式 (5.5.96) 关于 y_j 微分，由 (5.5.119) 可得

$$\frac{\partial f}{\partial y_j}+\sum_{k\geq j}\lambda_k*\frac{\partial h_k}{\partial y_j}=0 \quad 于(X^0,\lambda^0), \quad j\in M. \tag{5.5.127}$$

由 (5.5.124) 和 (5.5.126) 有

$$\lambda_j^0=0, \quad j\in M. \tag{5.5.128}$$

由于在 (X^0,Λ^0) 点也有 $\frac{\partial L}{\partial u_1}=0$, 这与下述方程矛盾：

$$\frac{\partial L}{\partial u_1}=\frac{\partial f}{\partial u_1}+\sum_{j\in M}\lambda_j*\frac{\partial h_j}{\partial u_1}.$$

由 (5.5.128) 及 (5.5.124) 知上式在 (X^0,Λ^0) 点为 1. 因此在此情形 $\widetilde{O}\mathrm{Zero}(LS/ISP)=\emptyset$. 而 (5.5.123) 通过下式由 (5.5.118) 容易得到

$$K\{x_1,ISP,O,HS\}=\emptyset \quad 对\ x_1=u_1. \tag{5.5.129}$$

考虑下一情形 $x_1=y_1$. 由 (5.5.120), 我们有

$$\frac{\partial f}{\partial y_1}=1, \quad \frac{\partial f}{\partial y_2}=\cdots=\frac{\partial f}{\partial y_r}=0. \tag{5.5.130}$$

再次令 (X^0,Λ^0) 是 $\widetilde{O}\mathrm{Zero}_{\mathbf{R}}(LS/ISP)$ 中任一零点. 如前, 由 (5.5.120) 及 (5.5.127) 可得

$$\begin{aligned}&\lambda_j^0=0, \quad j=2,\cdots,m,\\&\lambda_1^0=-\frac{1}{S_1^0}\neq 0,\end{aligned} \tag{5.5.131}$$

其中 S_1^0 是 S_1 在 X^0 点的值. 于是对任意 $j\in M$, 在 X_0 点有 $h_j=0$. 由于我们关于变量 X 选择的是自然序， h_1 将不含变量 u_j, 其是具有常系数仅含变量 $y_1=x_1$ 的多项式. 满足 $h_1=0$ 的可能的 x_1^0 的值的个数是有限的且包含在于 (5.5.116) 中 $h_1=0$ 的实数解集中. 由引理 5.5.19 知，集合 $\mathrm{Proj}_1\widetilde{O}\mathrm{Zero}_{\mathbf{R}}(LS/ISP)$ 是一有限集，也可能是空集，其中元素是满足 5.5.123 的实数. 那么 (5.5.122) 中的集合 K 可取为

$$\begin{aligned}K\{x_1,ISP,O,HS\}&=\mathrm{Proj}_1\widetilde{O}\mathrm{Zero}_{\mathbf{R}}(LS/ISP)\\&\subset \mathrm{Proj}_1 O\mathrm{Zero}_{\mathbf{R}}(h_1), \quad 其中\ x_1=y_1.\end{aligned} \tag{5.5.132}$$

引理 5.5.20 完全得证. □

一般情形下开区域上的有限核定理

现在考虑 HS 是含变量 $x_1, \cdots, x_n$ 的一般多项式的情形. 引入一新变量 x_0, 安排其序 $x_0 \prec x_1$, 并采用下述记号.

记号 5.5.21 $X^+ := (x_0, x_1, \cdots, x_n)$.

$\mathbf{R}^{n+1} := \mathbf{R}^{(n+1)}(X^+)$.

$O^+ := \mathbf{R}^{n+1}$ 中的开区域, 由 $X \in O$ 定义, 而 x^0 任意.

$\Lambda^+ := (\lambda_0, \lambda_1, \cdots, \lambda_m)$.

$\widetilde{O}^+ := O^+ \times \mathbf{R}^{m+1}(\Lambda^+)$.

$h_0 :=$ 新的多项式,

$$h_0(X^+) = f(X) - x_0. \tag{5.5.133}$$

$HS^+ :=$ 新的多项式集,

$$HS^+ := HS + \{h_0\}. \tag{5.5.134}$$

$g^+ :=$ 由 $g^+(X^+) = g(X)$ 定义的多项式.

$\text{Proj}_0 := \mathbf{R}^{n+1}(X^+)$ 到 $\mathbf{R}(x_0)$ 的自然投射.

下述引理显然成立.

引理 5.5.22

$$\{f(X)|X \in O\text{Zero}_{\mathbf{R}}(HS)\} = \text{Proj}_0 O^+\text{Zero}_{\mathbf{R}}(HS^+) \tag{5.5.135}$$

及

$$\text{EVal}_{\mathbf{R}}\{f, g, O, HS\} = \text{EVal}_{\mathbf{R}}\{x_0, g^+, O^+, HS^+\}. \tag{5.5.136}$$

定理 5.5.23 (开区域上的有限核定理) 令 HS 是多项式集, f 是 $\mathbf{R}[X]$ 中任一多项式, 那么存在一有限实数集 K, 使得

$$\text{EVal}_{\mathbf{R}}\{f, O, HS\} \subset K \subset \text{Proj}_0 \widetilde{O}^+\text{Zero}_{\mathbf{R}}(HS^+). \tag{5.5.137}$$

证明 由零点分解定理 3.5.2, 我们对 $\text{Zero}(HS^+)$ 作分解, 那么对一升列集 $HS_j^+ \subset \mathbf{R}[X^+]$, 其相应初式隔离子积是 ISP_j, 我们有

$$O^+\text{Zero}_{\mathbf{R}}(HS^+) = \bigcup_j O^+\text{Zero}_{\mathbf{R}}(HS_j^+/ISP_j). \tag{5.5.138}$$

令 LS_j^+ 是如引理 5.5.19 和 5.5.20 中由 HS_j^+ 构成的 Lagrange 多项式集. 由引理 5.5.20 以 x_0 代替 x_1, 则对任一 j 存在一有限实集 K_j, 使得

$$\mathrm{EVal}_{\mathbf{R}}\{x_0, ISP_j, O^+, HS_j^+\} \subset K_j \subset \mathrm{Proj}_0\widetilde{O}^+\mathrm{Zero}_{\mathbf{R}}(HS_j^+/ISP_j), \tag{5.5.139}$$

其中

$$K_j = K\{x_0, ISP_j, O^+, HS_j^+\}. \tag{5.5.140}$$

由 (5.5.138) 显然有

$$\mathrm{EVal}_{\mathbf{R}}\{x_0, O^+, HS^+\} \subset \bigcup_j \mathrm{EVal}_{\mathbf{R}}\{x_0, ISP_j, O^+, HS_j^+\}. \tag{5.5.141}$$

令

$$K = \bigcup_j K_j = \bigcup_j K\{x_0, ISP_j, O^+, HS_j^+\}, \tag{5.5.142}$$

由 (5.5.136) 及 (5.5.138)~(5.5.142), 我们有 (5.5.137). 定理得证. □

定义 5.5.24　给定 $\{f, O, HS\}$ 的问题 $\mathbf{E}$ 的 *有限核集* 是指 (5.5.142) 中有限核 K.

记号 5.5.25　$\mathrm{Ker}(f, O, HS) :=$ (5.5.142) 中的 $K :=$ 给定 $\{f, O, HS\}$ 的问题 $\mathbf{E}$ 的有限核集 K.

注释 5.5.26　如果在定理 5.5.23 中有 g 出现，该定理在略作修改后仍成立.

注释 5.5.27　定理 5.5.23 表明，虽然 $E\mathrm{Zero}_{\mathbf{R}}\{f, O, HS\}$ 可能是无限集，但

$$\mathrm{EVal}_{\mathbf{R}}\{f, O, HS\}$$

是一有限集.

注释 5.5.28　Lagrange 乘子法对任何可微函数 f, h_j 适用. 然而定理 5.5.23 所隐含的有限性质却不再成立. 这可由例子 $f = x*\sin(\frac{1}{x}), O = \{x > 0\} \subset \mathbf{R}^1(x)$ 看出. 因此，极值点集合的有限性是 f, h_j 为多项式时的特征.

例 5.5.29 (例 5.5.7 的改进)　再次考虑例 5.5.7. 此处我们有 $O = \mathbf{R}^2(x, y)$. 我们引进一新变量 x_0 并取 $h_0 = x^2 + y^2 - x_0$, 那么 $HS^+ = \{h_0, h_1\}$. 对序 $x_0 \prec x \prec y$, 容易发现

$$\mathrm{Zero}_{\mathbf{R}}(HS^+) = \mathrm{Zero}_{\mathbf{R}}(CS_1/ISP_1) + \mathrm{Zero}_{\mathbf{R}}(CS_2/ISP_2) + \mathrm{Zero}_{\mathbf{R}}(HS'),$$

右边的多项式及多项式集分别是

$$CS_1 = \{C_{11}, C_{12}\}, \quad CS_1 = \{C_{21}, C_{22}, C_{23}\}, \quad HS' = \{h_1', h_2', h_3'\},$$

而

$$C_{11} = x^3 - 2*x^2 + 3*x - x_0 - 1, \quad C_{12} = y^2 + x^2 - x_0,$$

$$C_{21} = x_0 - 1, \quad C_{22} = x - 1, \quad C_{23} = y,$$

$$h_1' = 3*x^2 - 4*x + 3, \quad h_2' = x^2 + y^2 - x_0, \quad h_3' = (x-1)^3 - y^2.$$

多项式 ISP_1, ISP_2 分别是 CS_1, CS_2 的初式隔离子之积. 因为 $h_1' = 0$ 没有实解, 所以 $\mathrm{Zero}_{\mathbf{R}}(HS') = \emptyset$. 其他两零点集对核集 $K\{f, \mathbf{R}^2, HS\}$ 的贡献分别由下式给出:

$$K_1 = \emptyset, \qquad K_2 = \{1\}.$$

因此有限核 $K = \{1\}$, 其是点 $(x_0, x, y) = (1, 1, 0)$ 到 $\mathbf{R}(x_0)$ 的投射, 所以唯一的极值 $f = 1$ 出现在唯一的极值点 $(x, y) = (1, 0)$.

闭域上的有限核定理

至今, 对问题 $\mathbf{E}(f, g, D, HS)$ 我们仅是限制在开集 $D = O$ 上考虑. 现在考虑闭域 D 的情形. 我们将仅限于考虑这样的闭域 D, 它的边界是由 $\mathbf{R}^n(X)$ 中的分片代数超曲面构成. 通过引进新变量及新的多项式, 通常我们可把域 D 转化成某高维实空间中的直角平行六面体. 因此不失一般性, 我们假设闭域 D 具有下述形式:

$$D : a_k \le x_k \le b_k, \quad k \in N = \{1, \cdots, n\}, \tag{5.5.143}$$

其中某些 a_k 或 b_k 可能是 $-\infty$ 或 $+\infty$, 此时忽略 $=$.

为把问题 $\mathbf{E}\{f, D, HS\}$ 转化成问题 $\mathbf{E}\{f, O, HS\}, O$ 是开集, 我们把域 D 分成至多 3^n 个某 n_τ 维实空间 $\mathbf{R}_\tau^{n_\tau}$ 中开区域 O_τ, 如下所示.

记号 5.5.30 $\tau :=$ 任一 n 元组 $(t_1, \cdots, t_n)$, 其中 t_k 是 $+, -$, 或 0.

$T :=$ 上述 n 元组的集合, 其满足若 $a_k = -\infty$, 则 $t_k \ne -$, 若 $b_k = +\infty$, 则 $t_k \ne +$.

下面 $f \in \mathbf{R}[X], HS \subset \mathbf{R}[X], \tau = (t_1, \cdots, t_n) \in T$:

$n_\tau := \tau$ 中 0 的个数.

$\mathbf{R}_\tau^{n_\tau} :=$ 如下定义的 $\mathbf{R}(X)$ 的子空间:

$$x_k = a_k \quad 对\ t_k = -,$$
$$x_k = b_k \quad 对\ t_k = +.$$

$O_\tau := \mathbf{R}_\tau^{n_\tau}$ 中开区域如下定义:

$$a_k < x_k < b_k \quad 对\ \tau_k = 0.$$

f_τ(或 h_τ) $:=$ f(或 h) 在 $\mathbf{R}_\tau^{n_\tau}$ 上的限制.

$HS_\tau :=$ 多项式 h_τ 的集合，其中 $h \in HS$.

下述引理是显然的.

引理 5.5.31 对某 $\tau \in T$, 如果 x 是 $O_\tau (\subset \mathbf{R}_\tau^{n_\tau})$ 中一点， x^τ 是其作为 $\mathbf{R}^n$ 空间点时的同一点. 那么

$$x^\tau \in E\text{Zero}_\mathbf{R}\{f, D, HS\} \Rightarrow x \in E\text{Zero}_\mathbf{R}\{f_\tau, O_\tau, HS_\tau\}.$$

从引理 5.5.31 可知

$$E\text{Zero}_\mathbf{R}\{f, D, HS\} \subset \bigcup_{\tau \in T} E\text{Zero}_\mathbf{R}\{f_\tau, O_\tau, HS_\tau\}. \tag{5.5.144}$$

现在应用定理 5.5.23 于 (5.5.144), 我们易得下面定理:

定理 5.5.32 (闭域上的有限核定理) 对问题 $\mathbf{E}\{f, D, HS\}$, 其中 D 是如 5.5.143 所示的闭域，存在一实有限核集 K, 使得

$$\text{EVal}_\mathbf{R}\{f, D, HS\} \subset K \subset \text{Proj}_0 O^+ \text{Zero}_\mathbf{R}(HS^+), \tag{5.5.145}$$

其中

$$K = \bigcup_{\tau \in T} K\{f_\tau, O_\tau, HS_\tau\}. \tag{5.5.146}$$

<u>*优化问题及优化原理*</u>

令 f, g, D, O, HS 仍如前所述.

定义 5.5.33 *最优* 是指最小或最大.

定义 5.5.34 f 在限制条件 $HS = 0, h \neq 0$ 下于区域 D 内的 *最优点* 是指点 $X^0 \in D\text{Zero}_\mathbf{R}(HS/g)$, 使得对任一点 $X' \in D\text{Zero}_\mathbf{R}(HS/g)$, 对于最优为最小时，总有 $f(X') \geq f(X^0)$, 或对于最优是最大时，总有 $f(X') \leq f(X^0)$.

定义 5.5.35 在限制条件 $HS = 0, h \neq 0$ 下，f 于域 D 内的 *最优值* 是指函数值 $f(X^0)$, 其中 X^0 是域 D 中满足限制条件 $HS = 0, g \neq 0$ 的任一最优点 (假设其存在).

记号 5.5.36 $\text{Optm}\{f, g, D, HS\} :=$ 在限制条件 $HS = 0$, $g \neq 0$ 下，f 于区域 D 内的最优 (最大或最小) 值 (假设其存在).

最优问题 O 在假设存在下，确定最优值 $\text{Optm}\{f, g, D, HS\}$.

每一最优点，无论最大或最小，显然都是相关问题的极值点. 这样，对最优点 (假设其存在) 的实际确定，我们有下述原理:

最优化原理 最优值 $\text{Optm}\{f,g,D,HS\}$(假设其存在) 是 $\text{EVal}_{\mathbf{R}}\{f,g,D,HS\}$ 的最优值.

对最优值, 无论最大或最小, 如果存在, 则由最优化原理确定最优值的问题可转化为确定某些更为确切的实子集上最优值, 这个子集甚至是有限的. 实际上, 由定理 5.5.15~5.5.32, 作为解决最优化问题的直接推论, 我们容易得到下述定理.

定理 5.5.37 对如 (5.5.143) 所示的开区域或闭域 D, 假设最优值存在, 我们有

$$\text{Optm}\{f,D,HS\} = \text{OptmKer}\{f,D,HS\}.$$

定理 5.5.38 假设最优值存在, 对于 D 是开区域 O, 我们有

$$\text{Optm}\{f,g,O,HS\} = \text{Optm}_{X\in O}\{f(X)|X \in LJZ\},$$

其中

$$LJZ = \text{LProj}\widetilde{O}\text{Zero}_{\mathbf{R}}(LS/g) + O\text{Zero}_{\mathbf{R}}(JS/g).$$

在最后表达式中, LS, JS 分别是问题 $E\{f,g,O,HS\}$ 的 Lagrange 多项式集及 Jacobi 多项式集.

第三部分　应用实例

第六章　在多项式方程组求解中的应用

§6.1　多项式方程组求解的基本原理：特征集方法

<u>§1.3 中 Descartes 方案的回顾</u>

在 §1.3 中我们引述了 Descartes 解决问题的方案，可简述如下：

求解任何问题 $\longrightarrow$ 求解数学问题
$\longrightarrow$ 求解代数问题
$\longrightarrow$ 求解代数方程组
$\longrightarrow$ 求解单个代数方程.

虽然 Descartes 方案表面上看来很荒唐，但是 Descartes 方案的重要性是毋庸置疑的. 事实上，近年来，多项式方程组求解在解决各种问题时都扮演着重要的角色，这一点已逐渐被科学界所认识. 有许多不同的方法可以用来处理多项式方程组 $PS=0$ 的求解问题，其中 $PS \subset \mathbf{K}[X], X=(x_1,\cdots,x_n)$, 并且 $\mathbf{K}$ 是特征为 0 的域，通常为有理数域 $\mathbf{Q}$.

<u>*多项式方程组求解的数值方法和符号方法*</u>

多项式方程组的求解主要有两种方法：数值方法和符号方法. 对于数值方法我们可以引述常用的 Newton-Raphson 方法以及它的不同的形式，同伦连续方法，等等. 这些方法从方程中已给定的数据出发，利用某种极限过程，期望收敛到给定的多项式方程组的某个解. 通常这种方法只能给出所有可能的解的集合中的一个解，因此主要是局部方法. 同伦连续方法，基于一些拓扑学上的考虑，在某些情形下能够给出所有可能解的集合，因此有时具有全局特征，这在特征值的确定方面是非常有效的. 同伦法的先驱之一李天岩已经向我们展示了该方法在某些一般问题中的正确性. 但无论如何，这些方法只能给出解的近似值，在误差控制和稳定性控制方面有一定问题. 与数值方法不同，符号方法将开始时的近似数据看做是未定元，因此在求解过程中只使用符号计算. 方程的解将以某种可接受的代数形式给出，所有可能的解都将以此形式表达，

于是这种方法具有全局特征．在符号方法中，我们特别地引述基于构造理想的 Gröbner 基的 Buchberger 方法，参见 [Bu1] 和如 [Kal], [Koba], [Laz1,2]．这种方法在零维情况下，即只存在有限多个解的情形，被证明是非常成功的．更一般的情形的研究正在进行中．

我们将采用符号计算方法．但我们的方法完全不同于 Buchberger 或其他的一些方法．我们把该方法称为特征集方法，事实上，它来源于中国古代关于求解多项式方程组问题的方法．

关于 §1.2 中中国古代多项式方程组求解方法的回顾

方程组求解是中国古代数学历史发展的主题．毫不夸张地说，我们古代数学的发展在不知不觉中遵循了 Descartes 方案，可以被看作 Descartes 方案的一种真正的实现．事实上，在公元前 2 世纪出现的，最早的名著《九章算术》中．通过引入负数，已经出现了解线性方程组的方法．这个方法与近代的 Gauss 消元法本质上是相同的． §1.2 中给出了一个具体的例子．按照现代的表示方法，这种方法是将给定的方程组约简为某种形式，该形式在现代定义中等价于如下所示的方程组：

$$\left.\begin{array}{l} c_{11} * x_1 + d_1 = 0, \\ c_{22} * x_2 + c_{21} * x_1 + d_2 = 0, \\ \cdots\cdots\cdots\cdots \\ c_{nn} * x_n + \cdots + c_{n1} * x_1 + d_n = 0, \end{array}\right\} \tag{6.1.1}$$

在以上的方程组中 (一些方程可能最终不会出现) 所有方程的首项系数 c_{ii} 是非零的，此时可以很容易求出方程组的解 (最终通过一些参数来表达，这些参数是没有出现的方程的主变元 x_i)．稍后，在公元 1303 年元朝朱世杰的著作《四元玉鉴》中给出了一种方法，这种方法描述了理论上求解一般非线性方程组的方法．该方法包括了化简给定的方程系统为某种容易求解的标准化形式．朱世杰方法的一个具体例子及其注释也在 §1.2 给出．由此，一个几何问题转化成一个包含三变元的三个多项式方程组，该多项式组在现代概念中被表示为 (1.2.11)，变元表示为 z, x, y．通过朱世杰的方法，这个多项式集合被约化成一个形如 (1.2.13) 的系统 (其中 x 假设非零)．在这个系统中，未定元 z, x, y 是被逐个引入．为了读者方便，我们将方程组 (1.2.13) 写成如下的形式：

$$\begin{array}{l} z^4 - 6 * z^3 + 4 * z^2 + 6 * z - 5 = 0, \\ x * (7 + 3 * z - z * * 2) - (6 + 7 * z + 3 * z^2 - z^3) = 0, \\ y - (x * z - x^2 - z + x) = 0. \end{array} \tag{6.1.2}$$

现在,对于每个单变元 z, x, 和 y 逐个求解上述方程组我们得到一组解 $(z, x, y) = (5, 3, 4)$. 如果需要, 可以利用公元 1247 年宋代秦九韶的方法求得所有实解. 我们看到, 虽然朱世杰的方法是不完全的, 并且由例 3.4.15 和 3.5.31 可以看出它是有缺陷的. 但是, 它提供了求解一般多项式方程组的思路.

由中国古代成就中得到的提示

方程组 (6.1.1) 和 (6.1.2) 提示我们引入如 §3.3 中的三角列和升列的概念. 我们以略微不同的方式重述这些概念如下:

我们考虑一个具有特殊形式的多项式集合 $AS \subset \mathbf{K}[X]$. 假设未定元 $x_1, \cdots, x_n$ 被重新排列为 $u_1, \cdots, u_d, y_1, \cdots, y_r$ $(r+d=n)$, 使得 AS 中的多项式 $A_1, \cdots, A_r$ 可以被重排为如下的规范形式:

$$\left.\begin{array}{rcl} A_1 &=& I_1 * y_1^{d_1} + \text{关于 } y_1 \text{ 的低次项}, \\ A_2 &=& I_2 * y_2^{d_2} + \text{关于 } y_2 \text{ 的低次项}, \\ && \cdots\cdots\cdots\cdots \\ A_r &=& I_r * y_r^{d_r} + \text{关于 } y_r \text{ 的低次项}. \end{array}\right\} \tag{6.1.3}$$

在 (6.1.3) 中, 对于每一个 i, A_i 中关于 y_i 幂次的系数是 $\mathbf{K}[u_1, \cdots, u_d, y_1, \cdots, y_{i-1}]$ 中的多项式. 此时多项式集合 AS 是一个三角列. 进而, 如果每一个多项式 I_i 关于 y_j $(j < i)$ 的次数小于 $deg(A_j) = d_j$, 那么多项式集合 AS 是一个升列. 多项式 I_i 被称做初式, $IP = \Pi\, I_i$ 称做 AS 的初式积.

多项式方程组求解的原理

显然, 由 (6.1.3) 定义的一个三角列或者一个升列正好是出现在 (6.1.1) 和 (6.1.2) 的左半部的多项式的一般形式. 我们解释一下多项式方程组求解的简单原理:

原理 PES. 考虑形如 $AS = 0$ 的多项式方程组的求解, 其中 AS 是形如 (6.1.3) 的三角列或者升列. 因为未定元 $y_1, \cdots, y_r$ 是由 $u_1, \cdots, u_d$ 确定的代数函数, 而且所有的初式都不为零, AS 可以被认为求解完毕. 如果知道 u 取确定值, 那么在初式不为零时, y 的值作为方程的解也确定了. 换言之, $\text{Zero}(AS/IP)$, 或更一般地, $\text{Zero}(AS/IP * G)$, 其中 $G \in \mathbf{K}[X]$, 可以被认为是一个可确定的集合.

上面的简单原理给我们提供了解决任意形如 $PS = 0$ 的多项式方程组的思路, 并把它简化为下面的问题:

问题 PES1. 由给定的多项式集合 PS 计算出一个三角列或升列 AS,使得 AS 的零点集与 PS 的零点集密切相关, 这给出了 $\text{Zero}(PS)$ 的重要部分的部

分确定. 由此, 可以完全确定 $\text{Zero}(PS)$.

问题 PES2. 由给定的多项式集合 PS, 计算出一个升列的集合 (或三角列集合) AS_i, 使得 PS 的零点集可以通过升列集 (或三角列集) AS_i 的零点集所确定.

多项式方程组求解的特征列方法

沿着我们先人提供的思路, 主要借鉴了 J. F. Ritt 的两本现代数学经典著作 [Ritt1,2], 我们将引入严格的概念和技术. 其目的在于重新表述 1303 年朱世杰的工作并将之严格化, 精确化. 由此, 我们得到 §3.4 的整序原理和 §3.5 的零点分解定理中描述的特征列方法. 它们至少在理论上彻底解决了 PES1 和 PES2 这两个问题, 这里将它们重述如下:

整序原理 对于给定的多项式集合 PS, 存在算法在有限步内确定一个特殊的升列 CS, 称做 PS 的特征列, 使得

$$\text{Zero}(PS) = \text{Zero}(CS/IP) + \bigcup_i \text{Zero}(PS_i), \tag{6.1.4}$$

其中

$$PS_i = PS + CS + I_i \text{ 或 } PS + I_i, \tag{6.1.5}$$

IP 是 CS 的初式积, 即 CS 的所有初式 I_i 的乘积.

零点分解定理 对于给定的多项式集合 PS, 存在算法确定一个有限的升列集合 (或三角列集合) AS_j, 使得

$$\text{Zero}(PS) = \bigcup_j \text{Zero}(AS_j/IP_j), \tag{6.1.6}$$

其中每一个 IP_j 是对应的升列 (或三角列)AS_j 的初式的乘积.

我们在第三章还给出不同形式的零点分解定理. 有了上述两个定理, 多项式方程组求解问题至少在理论上已经完全解决了.

一般二次方程系统的示例

为了演示特征列方法在多项式方程组求解中的作用, 我们看下面的示例:

例 6.1.1 设 PS 是由三个一般的二次多项式 P_j 组成的多项式集合, 未定元是 x_1, x_2, x_3:

$$P_j = \sum c^j_{ghk} * x_3^g * x_2^h * x_1^k, \ j = 1, 2, 3. \tag{6.1.7}$$

在每个 P_j 的求和运算中 g, h, k 遍历所有使得 $g + h + k \leq 2$ 的非负整数. 其中 c^j_{ghk} 被看作常数未定元.

根据 §3.4 的方案 (S) 中的 $PS_i = BS_{i-1}+RS_{i-1}$ 所示, 令初始的 $PS = PS_0$, 利用我们的算法我们相继地得到多项式集合 PS_i 如下所示:

$$\begin{aligned}
&PS_0 : [10\ x_3\ 2],\ [10\ x_3\ 2],\ [10\ x_3\ 2],\\
&PS_1 : [18\ x_3\ 1],\ [18\ x_3\ 1],\ [10\ x_3\ 2],\\
&PS_2 : [108\ x_2\ 3],\ [258\ x_2\ 4],\ [18\ x_3\ 1],\\
&PS_3 : [16211\ x_2\ 2],\ [108\ x_2\ 3],\ [18\ x_3\ 1].
\end{aligned}$$

下一步我们不得不构造 PS_3 中指标集为 $[16211\ x_2\ 2], [108\ x_2\ 3]$ 的两个多项式的余式. 但是这超出了我们的计算机 SUN3/140 的能力. 甚至一台更大的计算机看起来也很难把这样的计算完成.

<u>特征列方法中项数和次数的膨胀</u>

上述的例子说明 §3.4 的方案 (S) 中给出的算法在运行过程中出现的多项式的项数可能增长很快, 以至于难以控制. 事实上, 对于两个多项式 $P_1, P_2 \subset \mathbf{K}[X]$, 各自的项数分别是 t_1, t_2, 它们的乘积 $P_1 * P_2$ 的项数可能会增长到 $t_1 * t_2$. 此外, 余式的形成是运算过程中用到的基本操作, 这项操作本身包括如下类型的更基本的操作: 考虑两个多项式 P_1, P_2 具有相同的类 $c > 0$ 并且各自具有次数 d_1, d_2. 将 $P_i (i = 1, 2)$ 记为形式 $P_i = I_i * x_c^{d_i} + P_i'$ 并且假设 $d_1 \geq d_2$, I_i 是 P_i 的初式, 使得 P_i' 的类或者小于 $< c$ 或者等于 c, 同时次数 $< d_i$, 则基本操作包括构造多项式 $P_3 = I_2 * P_1' - I_1 * P_2' * x_c^{d_1 - d_2}$. 令 t_{i1}, t_{i2}, t_1, t_2 是 I_1, I_2, P_1, P_2 的相应的项数. P_3 的项数可能增加到 $t_{i2} * (t_1 - t_{i1}) + t_{i1} * (t_2 - t_{i2})$. 更为严重的是 P_3 中变元 $x_j (j < c)$ 的次数可能增加到 $d_{j1} + d_{j2}'$ 或者 $d_{j1}' + d_{j2}$, 如果 $d_{j1}, d_{j2}, d_{j1}', d_{j2}'$ 是 I_1, I_2, P_1', P_2' 中对于 x_j 各自的次数, 则这种次数的增长将导致后面运算中的极大困难.

<u>特征列方法中的 Collins- 李现象</u>

另外, 这种方法也有其他的不足. 例如, 我们考虑两个多项式 $P_1, P_2 \subset \mathbf{K}[X]$, 它们具有相同的类 c 和次数 $d_1 \geq d_2$. 我们可以构造一系列的多项式

$$P_1, P_2, \cdots, P_k, \cdots$$

其中每一个 $P_i\ (i \geq 3)$ 是 P_{i-2} 对于 P_{i-1} 的余式, 这里的多项式都是以 x_c 为变量的多项式. Collins 证明了当余式是伪余式时, 上面序列的后面的多项式从某一点向后将不可避免的包括前面多项式的初式做因子. 如果余式的概念按照 Ritt 的理解给出, 那么结论仍然正确. 作为上述由 Collins 所发现的现象的推广, 李子明证明了在 §3.4 的方案 (S) 的运算中将不可避免地出现不必要的、

多余的因子，这些因子是前面得到的各种各样的基列 BS 的初式. 这些因子的出现使得出现在程序中的多项式变得极大以至于难以计算，比应该得到的形式复杂得多. 也有可能出现其他类型的不希望得到的、原因不明的因子. 为了弥补这种现象所产生的项数和次数的膨胀，我们必须通过简单的除法，将程序中出现的多项式尽可能的分解成因子，来去掉所有这些不希望出现的初式因子. 这样的操作对于解的影响可以由下面的公式给出：

$$\begin{aligned}&\mathrm{Zero}(PS) = \mathrm{Zero}(PS/F) + \mathrm{Zero}(PS + \{F\}),\\ &\mathrm{Zero}(PS + \{F_1 * F_2\}) = \mathrm{Zero}(PS + \{F_1\}) + \mathrm{Zero}(PS + \{F_2\}).\end{aligned} \tag{6.1.8}$$

基于以上的研究，由王定康在 SUN SPARC2 工作站上开发了一个名为 wsolve 的软件包. 这个软件包对于多项式方程组求解相当有效，并可以解决许多有趣的问题. 这些问题我们将在后面的章节看到它们.

系数的系统化的压缩形式

一个部分控制项数膨胀的方法是压缩系数的方法. 为此，我们将首先引入一些关于多项式和系数的符号.

令给定的多项式集合 $PS \subset \mathbf{K}[X]$ 由多项式 $P_1, \cdots, P_k$ 组成. 从 PS 出发我们根据 §3.4 和 §3.5 的构造余式或替代规则的算法相继地得到多项式 P_{k+1}, P_{k+2} 等等. 对于此序列中的某个多项式 P_j，我们将用 c_t^j 表示单项式

$$X^t = x_n^{d_n} * \cdots * x_1^{d_1},$$

的系数，其中 $t = (d_n, \cdots, d_1)$. 我们将多项式 P_j 中有相同部分 $X^u (u = (d_n, \cdots, d_k)$ 或 $(d_n, \cdots, d_k, 0, \cdots, 0)$，即最后 $k-1$ 个分量为 0，$k > 1)$ 的项合并成一项. 相应的 X^u 的系数由 c_u^j 表示，使得

$$c_u^j = \sum_v c_{uv}^j * X'^v,$$

这里 $X' = (x_{k-1}, \cdots, x_1)$，同时求和运算将遍历所有可能的整元组 $v = (d_{k-1}, \cdots, d_1)$. 自此像 c_u^j 或 c_{uv}^j 这样的系数将被称为相应多项式的压缩系数. 因此，为了突出例 6.1.1 里 P_j 中 x_3 的重要性，我们可以将其写成如下形式：

$$P_j = c_2^j * x_3^2 + c_1^j * x_3 + c_0^j, \ j = 1, 2, 3, \tag{6.1.9}$$

其中

$$\left.\begin{aligned}&c_2^j = c_{200}^j,\ c_1^j = c_{11}^j * x_2 + c_{10}^j,\ c_0^j = c_{020}^j * x_2^2 + c_{01}^j * x_2 + c_{00}^j,\\ &c_{11}^j = c_{110}^j,\ c_{10}^j = c_{101}^j * x_1 + c_{100}^j,\ c_{01}^j = c_{011}^j * x_1 + c_{010}^j,\\ &c_{00}^j = c_{002}^j * x_1^2 + c_{001}^j * x_1 + c_{000}^j.\end{aligned}\right\} \tag{6.1.10}$$

关于压缩系数方法的一个示例

例 6.1.2　我们再次考虑例 6.1.1, 假设系数 c^j $(j=1,2,3)$ 是相互独立的常变量. 经过压缩技术处理, 多项式集合 $PS=PS_0=\{P_1,P_2,P_3\}$ 被看作与系统 $PS_1=\{P_4,P_5,P_6\}$ 是 0 等价的, 其中 P_4,P_5,P_6 由以下形式给出:

$$\left.\begin{aligned}P_4&=x_3^2+c_{10}^4*x_3+c_{02}^4*x_2^2+c_{01}^4*x_2+c_{00}^4,\\P_5&=x_3*x_2+c_{10}^5*x_3+c_{02}^5*x_2^2+c_{01}^5*x_2+c_{00}^5,\\P_6&=c_{10}^6*x_3+c_{02}^6*x_2^2+c_{01}^6*x_2+c_{00}^6.\end{aligned}\right\}\tag{6.1.11}$$

在 (6.1.11) 中, 对 $i=4,5,6$ 我们有

$$\left.\begin{aligned}&c_{10}^i=c_{101}^i*x_1+c_{100}^i,\\&c_{02}^i=c_{020}^i,\ c_{01}^i=c_{011}^i*x_1+c_{010}^i,\\&c_{00}^i=c_{002}^i*x_1^2+c_{001}^i*x_1+c_{000}^i.\end{aligned}\right\}\tag{6.1.12}$$

注意到所有的 $c^i(i=4,5,6)$ 都是 $c^j(j=1,2,3)$ 的确定的有理函数. 为简单起见, 我们将在以后把 $c_{ghk}^i(i=4,5,6)$ 看作独立未定元.

从现在开始 P_4,P_5 对于 P_6 的余式都看作关于 x_3 的多项式. 我们得到两个多项式

$$\left.\begin{aligned}P_7&=c_{030}^7*x_2^3+c_{02}^7*x_2^2+c_{01}^7*x_2+c_{00}^7,\\P_8&=c_{040}^8*x_2^4+c_{03}^8*x_2^3+c_{02}^8*x_2^2+c_{01}^8*x_2+c_{00}^8.\end{aligned}\right\}\tag{6.1.13}$$

在 (6.1.13) 中, 我们有

$$\left.\begin{aligned}c_{030}^7&=-\,c_{02}^6,\\c_{02}^7&=c_{10}^6*c_{02}^5-c_{02}^6*c_{10}^5-c_{01}^6,\\c_{01}^7&=c_{10}^6*c_{01}^5-c_{01}^6*c_{10}^5-c_{00}^6,\\c_{00}^7&=c_{10}^6*c_{00}^5-c_{00}^6*c_{10}^5.\end{aligned}\right\}\tag{6.1.14}$$

$$\left.\begin{aligned}c_{040}^8&=(c_{02}^6)^2,\\c_{03}^8&=2*c_{02}^6*c_{01}^6,\\c_{02}^8&=(c_{10}^6)^2*c_{02}^4-c_{10}^6*c_{02}^6*c_{10}^4+2*c_{02}^6*c_{00}^6+(c_{01}^6)^2,\\c_{01}^8&=(c_{10}^6)^2*c_{01}^4-c_{10}^6*c_{01}^6*c_{10}^4+2*c_{01}^6*c_{00}^6,\\c_{00}^8&=(c_{10}^6)^2*c_{00}^4-c_{10}^6*c_{00}^6*c_{10}^4+(c_{00}^6)^2.\end{aligned}\right\}\tag{6.1.15}$$

方程 (6.1.14) 和 (6.1.15) 表示前面的多项式的压缩系数, 称为辅助方程组. 现在对 P_7,P_8 使用 §3.5 的替换规则, 我们得到类为 2, 次数为 1 的消元式 P_9, 和一个关于变量 x_2 的结式. 通过辅助方程 (6.1.14), (6.1.15) 将 P_9,P_{10} 中所有的 c 用 c^i 的项表示, 其中 $i=4,5,6$, 我们得出 P_9 和 P_{10} 中形如 c_{02}^6 的因子

$$c_{10}^6 = c_{101}^6 * x_1 + c_{100}^6.$$

除去这些因子所得到的商多项式仍然用 P_9, P_{10} 表示. 如果我们依照 (6.1.12) 进一步展开 P_9, P_{10}, 那么 P_9, P_{10} 的指标集分别为 $[1503\ x_2\ 1]$ 和 $[34411\ x_1\ 8]$. 经确认我们看到 P_4, P_5, P_6 对于升列 $CS = \{P_{10}, P_9, P_6\}$ 的余式都是 0. 由此推出 CS 是 $PS_1 = \{P_4, P_5, P_6\}$ 的一个特征列, 从而也是 $PS = \{P_1, P_2, P_3\}$ 的一个特征列. 除去的因子 c_{02}^6 和 c_{10}^6 是因为我们把它们看作是非零的. 注意如果我们用 P_1, P_2, P_3 的初始系数表示 CS 的多项式的系数并且除掉分母, 那么项数将达到十亿阶.

注意在这个过程中我们消去了因子 c_{02}^6, c_{10}^6. 作为一个非零常数的第一个因子的消去是不重要的, 但是第二个因子的消去告诉我们整序原理和 (6.1.8) 蕴涵恒等式

$$\text{Zero}(PS) = \text{Zero}(CS/IP * c_{10}^6) + \text{Zero}(PS + \{IP\}\ /\ c_{10}^6) + \text{Zero}(PS + \{c_{10}^6\}).$$

因为我们假设 $c^j (j = 4, 5, 6)$ 是独立未定元, 那么很容易确定 P_9 和 P_{10} 是不可约的. 通过简单的推理, 得到上述的恒等式将可以简化为

$$\text{Zero}(PS) = \text{Zero}(CS). \tag{6.1.16}$$

Czapor 和 Geddes 的进一步示例

例 6.1.3 作为一个进一步的例子, 我们考虑例 3.4.21 和 4.3.24 中 Czapor 和 Geddes 的多项式方程组的求解, 即 $PS = 0$, 其中未定元是 x, y, z, 这里 PS 是由如下三个多项式组成的:

$$\left.\begin{aligned} P_1 &= x^2 + a * y * z + d * x + g, \\ P_2 &= y^2 + b * z * x + e * y + h, \\ P_3 &= z^2 + c * x * y + f * z + k. \end{aligned}\right\} \tag{6.1.17}$$

其中变量 $a, \cdots, k$ 被看作独立常变量, 未定元 x, y, z 恰好是前面的 x_1, x_2, x_3, 但是我们将保留当前的符号. 我们看到如果我们设

$$x_1 = x,\ x_2 = y,\ x_3 = z,$$

及

$$\left.\begin{aligned} &c_{11}^4 = 0,\ c_{10}^4 = f,\ c_{02}^4 = 0,\ c_{01}^4 = c * x,\ c_{00}^4 = k; \\ &c_{10}^5 = 0,\ c_{02}^5 = 0,\ c_{01}^5 = 0,\ c_{00}^5 = (x^2 + d * x + g)/a; \\ &c_{10}^6 = b * x,\ c_{02}^6 = 1,\ c_{01}^6 = e,\ c_{00}^6 = h, \end{aligned}\right\} \tag{6.1.18}$$

(6.1.17) 中的 P_1, P_2, P_3 已经具有 (6.1.11) 中 P_5, P_6, P_4 的形式.

利用 (6.1.15) 的值我们看到例 6.1.2 中的 P_9, P_{10} 变成了各自项数为 137 和 35 的多项式. 因此, 如同例 3.4.21, (6.1.17) 中的多项式集合 $PS = \{P_1, P_2, P_3\}$ 有一个指标集为 $[137\ x\ 8], [35\ y\ 1], [4\ z\ 1]$ 的特征列 CS 和 $\mathrm{Zero}(PS) = \mathrm{Zero}(CS)$.

<u>若干结论性注释</u>

注释 6.1.4 让我们用 $maxt$ 来表示出现在利用特征集方法或其他方法求解过程中的多项式的项数的最大值. 那么在例 6.1.3 中整个求解过程中的所有多项式的项数比较小, 为 $maxt = 324$. 同时计算也非常简单. 根本的原因在于不仅我们忽略了所有多余因子的出现, 而且我们根据 §3.5 的命题 3.5.9, 3.5.10 和 3.5.13, 利用辅助方程组将前面所有的在相继的多项式集合中出现的多项式表示成压缩系数的形式.

注释 6.1.5 上述简化系数的方法的一个重大缺陷在于: 一个普通的非压缩形式的多项式可能出现这些因子. 如果需要的话, 可以用现在的软件检测出来并除去. 但是, 当多项式化为压缩系数的形式, 通常不可再分解, 所以没有办法检测出这样的可能出现的因子.

注释 6.1.6 采用人机交换的方法进行计算, 我们可以通过观察, 从而采用一些特殊的方法和技巧来控制多项式的项数. 例如, 我们可以用某个与多项式集合 PS 中的多项式 P, Q 0- 等价 的 P', Q' 替代 P, Q, 其中 P', Q' 是 P, Q 的线性组合使得由此得到的新的多项式集合 PS' 的零点集变得容易确定.

注释 6.1.7 即使我们尽可能的除去了多余的因子, 并且使用了一些特殊的方法, 但是在求解过程中出现的多项式仍然有可能变得太大以至于无法进行下一步的计算. 在符号计算中由于参数的一般性, 上述现象的出现是不可避免的. 看起来唯一的办法是利用一种混合的办法将符号计算与数值计算的方法联系起来, 特别是对于一些特殊的应用. 但是我们将把这个问题留到下一节.

§6.2 一种多项式方程组求解的混合方法

<u>多项式方程组求解的一种混合方法的必要性</u>

我们从上一节知道, 多项式方程组求解有两种方法: 符号计算方法和数值计算方法. 除非特别声明, 基域 $\mathbf{K}$ 被理解为 $\mathbf{R}$ 或 $\mathbf{C}$. 两种方法有各自的优点和缺点. 与数值计算方法不同, 符号计算方法在精确性上有优势. 但是考虑解决一个包含三个二次方程的简单问题, 变元是 x, y, z, 无论这些方程的系数是参数还是近似的数值, 对于符号计算方法我们不得不用变量替代这些数字的

值. 如例 6.1.1 和 6.1.2 所示, 我们发现最后的方程组, 即只包含变元 x 的方程组, 将很难确定或者将因为项数太大而令人失去兴趣或没有实用价值. 因此, 符号计算方法具有在计算过程中有可能产生非常大的多项式的缺点. 但是, 如果我们用给定的多项式的初始值替代中间系数, 那么最后变元是 x 的次数为 8 的多项式在最坏的情形下可能只有 9 项. 这表明了符号计算方法可能是非常不实用的, 特别是对于实际中的问题. 另一方面通常用的数值计算方法几乎不能给出所有可能的解. 因此, 看起来一种解决的办法就是使用一种混合方法, 保持符号计算和数值计算两种方法的优点并避开两种方法的不足.

混合方法的困难

注意如果我们在使用符号计算方法解方程组时使用数值系数, 那么在计算过程中系数会出现误差累加, 这种误差会导致最后结果不可靠. 同时也要注意在符号计算方法中因式分解是不可避免的, 但是以近似数值为系数的多项式的因式分解缺乏确切的含义. 因此为了给出令人满意的多项式方程组求解的混合方法, 我们必须先解决下面两个问题:

问题 H1. 在混合计算过程中的误差估计和误差控制.

问题 H2. 近似数值系数的多项式的因式分解.

这两个问题将在下面分开论述.

一个数字代数方程的根的估计

众所周知一个单变元的多项式方程的根对于系数是连续的, 根对于系数的轻微扰动是很敏感的. 为准确起见, 我们引用下面 Ostrowski 的一个定理:

定理 6.2.1 考虑两个多项式

$$f(z) = a_0 * z^n + \cdots + a_n, \tag{6.2.19}$$

$$g(z) = b_0 * z^n + \cdots + b_n. \tag{6.2.20}$$

假设 $a_0 * a_n \neq 0$ 并且设 $f(z) = 0$ 的根是 $z_1, \cdots, z_n$. 假设存在一个正数 τ 满足

$$4 * n * \tau^{\frac{1}{n}} \leq 1, \tag{6.2.21}$$

且对于 $i = 1, \cdots, n$,

$$|b_i - a_i| \leq |a_i| * \tau, \tag{6.2.22}$$

则可以适当排列 $g(z) = 0$ 的 n 个根 $y_1, \cdots, y_n$, 使得对于每一个 $i = 1, \cdots, n$,

$$\left|\frac{y_i}{z_i} - 1\right| < 8 * n * \tau^{\frac{1}{n}}. \tag{6.2.23}$$

定理表明了对于一个次数是 4 的方程，为了把根精确到小数点后两位，需要把方程的系数精确到小数点后 8 位或更多．有例子显示这样的误差估计是不可能改进的．因此，误差估计似乎没有实际用处．尽管如此，我们也没有理由气馁．参见 Ostrowski 在 [O2], p.111 和 p.221 中的讨论．

近似数字的准确表示

从现在开始，我们设基域 $\mathbf{K}=\mathbf{R}$, $\mathbf{K}=\mathbf{C}$ 的情形可以类似处理．

为了达到目的，我们将以下面的方式讨论问题．对于一个近似值 a, 我们把它写为 a_0+t_0, 这里 a_0 是一个已知的准确的逼近 a 的有理数，而 t_0 是一个充分小的未知的但准确的数．例如，我们可以把 π 写成 $\pi=\frac{31416}{10000}+t$ 的形式，这里 $\frac{31416}{10000}$ 和 t 都是准确的数，t 是一个未知数，它的量级 $|t|<10^{-4}$.

定义 6.2.2 一个近似数 a 的准确表示是指 a_0+t_0, 其中 a_0 是一个已知的准确的有理数，并且 t_0 是一个未知的准确的数，其中 $|t_0|<10^{-N}, N$ 是一个正整数．

定义 6.2.3 按照上面的定义，在准确表示 $a=a_0+t_0$ 中，a_0 称为 a 的基本部分，t_0 称为 a 的微小部分，N 为这种表示的精度次数．

含有近似系数的多项式的准确表示

让我们考虑多项式方程组 $PS=0$, 其中 $PS\subset\mathbf{R}[x_1,\cdots,x_n]$.

定义 6.2.4 多项式集 PS 的精确次数为 N 的准确表示是指将 PS 中任意多项式的每一个近似数值系数 c_i 用它的满足预先给定的精度次数为 N 的准确表示 $c_{i0}+t_i$ 替代，得到 PS 中多项式的新的表达形式，其中 c_{i0} 是基本部分，t_i 是微小部分，这样得到的多项式满足所有 $|t_i|<10^{-N}$.

定义 6.2.5 根据上面定义的 PS 的准确表示，t_i 称为微小部分，N 为这种表示的精确次数，k 个微小部分的积的任意的有理线性组合称为一个 k 阶微小部分．

多项式方程组求解的混合方法

现在我们用下面的方法求解含有近似数值系数的方程组 $PS=0$. 首先，固定一个精度次数 N 和一个正整数 s. 把给定的多项式集合转化成它的准确表示，仍然用 PS 表示．现在，用某种符号计算方法求解 $PS=0$, 比如说特征列方法．为了确定 PS 的一个特征列 CS, 让我们利用常规的特征列算法．在这个过程中，我们将把阶数大于 s 的微小部分置为 0. 因此，设特征列 CS 的第一个多项式为

$$C_1=(a_0+T_0)*x_1^n+\cdots+(a_n+T_n), \tag{6.2.24}$$

在这里 T_k 是阶数小于或等于 s 的微小部分, a_k 是准确的已知有理数. 对其他的特征列 C_i 也是相同的.

定义 6.2.6 上面得到的多项式集合 $\{C_i\}$ 称为给定多项式 PS 的阶数为 s 的近似特征列.

同样地, 使用 §3.4 和 §3.5 中其他的方法, 我们可以得到近似特征级数, Zero(PS) 的近似零点分解等等. 这里我们不再深入讨论.

假设 (6.2.24) 中 $a_0 * a_n \neq 0$. 令 C_{10} 给定如下:

$$C_{10} = a_0 * x_1^n + \cdots + a_n. \tag{6.2.25}$$

我们同样地处理其他的多项式 C_i 得到多项式 C_{i0}. 现在我们用 $C_{10} = 0$ 替代方程组 (6.2.24) $C_1 = 0$, 来求解方程组 (6.2.25). 然后, 相继求得其他的多项式 $C_{i0} = 0$. 利用 Ostrowski 的定理可以给出解的一个粗略的误差估计. 因此, 上述定理给出了一个多项式方程组求解的混合方法, 并且 Ostrowski 定理给出了粗略的误差估计.

注释 6.2.7 为了得到 (6.2.25), 我们必须把多项式方程组 $PS = 0$ 的每一个数值系数 c_i 替换为它的准确形式 $c_{i0} + t_i$ 两项. 因此, 在得到特征列 CS 的过程中出现的多项式可能会非常大, 以至于计算变得非常复杂而难以进行. 但是, 对于在此过程中出现的每一个多项式, 我们只保留 t_i 中次数 $\leq s$ 的项. 因此, 如果 t_i 的数量是 m, 那么 C_{10} 的项数将最多在 $s = 1$ 时达到 $(n+1)*(m+1)$, 在 $s = 2$ 时达到 $(n+1)*(1+m*\frac{m+3}{2})$. 对于求解过程中出现的其他多项式也是同样的. 用这种方法, 多项式将被控制在一个合理的项数范围, 并且计算可以在没有多大困难的情况下进行.

注释 6.2.8 如前所述, 在用 $C_{10} = 0$ 替代求解 $C_1 = 0$ 和其他方程的过程中, 为了得到低次精度, 需要有高精度的系数 a_i, 为此, 需要高精度的原始系数. 这意味着开始时的精确次数 N 应该选得足够高. 但是, 在使用上面的方法时, 这个缺点恰恰变成了优点. 因为如果 t_i 的量级为 $< 10^{-N}$, 那么, 形如 $t_i * t_j$ 和 $t_i * t_j * t_k$ 的乘积的量级将分别 $< 10^{-2*N}$ 和 10^{-3*N}. 因此, N 的选取足够大可以保证我们安全的忽略 t_i 中次数 ≥ 3 或 ≥ 2 的项.

注释 6.2.9 假设在此过程中任何初式的基本部分都不会变成 0, 那么上面的混合方法将没有理论上的困难, 并且 Ostrowski 定理至少在理论上提供了误差估计和误差控制的方法. 但是, 我们还不清楚在什么情况下运算过程中的某些初式的基本部分会变成 0. 而在下面我们会看到在实际情况中很少会出现这种情况.

注释 6.2.10　对于一些数 $a+\sum_k b_k*T_k$, 其中 T_k 是出现在运算过程中的 k 个微小部分的乘积，微小部分 T_k 的一些系数 b_k 可能与 a 相比是足够大的，这使得 b_k*T_k 看上去不再是微小的的数. 但是，这样的错误可以由充分地提高精确度来弥补. 另一方面，它表明了我们经常使用的那种直接在计算中使用近似数值的方法，即把所有的 t_i 置为 0 的方法，在理论上是不可靠的.

<u>数值系数的健康的和病态的近似</u>

下面，我们将阐述如何处理注释 6.2.9 中所阐述的特征列方法中的数值系数的准确表示所带来的困难. 为此，我们考虑一个多项式集合 $PS\subset \mathbf{R}[x_1,\cdots,x_n]$, 它的零点集待定. 首先，根据 §3.3 的方案 (S) 中的特征列方法确定 PS 的特征列. 先把 PS 中的多项式的近似数值看作独立未定元. 按照 §3.3 中方案 (S) 的过程，根据它出现的序我们排列给定的多项式集合 PS 的多项式，并相继引入非零余式序列

$$P_1,P_2,\cdots,P_M. \tag{6.2.26}$$

现在让我们固定一个精确度 N, 并且对每一个近似数值系数 c_i, 我们用它的准确表示 $c_{i0}+t_i$ 来代替，保证每一个精确度 $N'>N$, 其中 c_{i0} 是基本部分，t_i 是相应的微小部分. 像前面一样，我们用同一种方法处理，将微小部分 t_i 看作独立未定元，并且根据它出现的序我们排列给定的多项式集合 PS 中的多项式，并相继引入非零余式序列. 我们将得到如下的一个多项式序列:

$$P_1',P_2',\cdots,P_M'. \tag{6.2.27}$$

显然，它和前面的多项式序列是一一对应的. 事实上，每一个由 P_k 得到的相应的 P_k' 就是将 P_k 中每一个未定的 c_i 用它的准确表示 $c_{i0}+t_i$ 替代.

定义 6.2.11　一个准确表示 $c_i=c_{i0}+t_i$ 称为是 k 级病态的当且仅当序列 (6.2.27) 中的 P_k' 的某个关于 $x_1,\cdots,x_n$ 的单项式的系数是微小部分的多项式，其中不包括微小部分等于 0 的部分. 这时，该单项式称为病态单项式.

定义 6.2.12　一个准确表示 $c_i=c_{i0}+t_i$ 是健康的当且仅当在序列 (6.2.27) 中不是任何级病态的.

假设对于准确表示 $c_i=c_{i0}+t_i$, 序列 (6.2.27) 开始时是 k 阶病态的. 如果我们设某阶的微小部分为 0, 并且按照前面的方法处理，那么，后面的多项式可能会出现与 (6.2.26) 或 (6.2.27) 完全不同的形式. 因此，最终得到的特征列与 (6.2.26) 或 (6.2.27) 的有本质的不同，从而完全不可靠. 另一方面，如果准确表达是健康的，尽管我们在求解的过程中将所有的微小部分置为 0, 但是我

们可以如前处理, 同样可以得到与利用 (6.2.26) 或 (6.2.27) 得到的有相同形式的序列, 并得到与利用 (6.2.26) 或 (6.2.27) 得到的形式相同的近似特征列. 因此, 问题简化为寻找多项式集合 PS 的、给定精确度 N 的、近似数值系数的健康表示. 我们需要如下引理.

引理 6.2.13 给定关于 $t_i(i=1,\cdots,r)$ 的有限的多项式集合 $\mathcal{P}$ 和足够小的 $\epsilon>0$, 在实空间 $\mathbf{R}^r(t_1,\cdots,t_r)$ 的原点 $(0,\cdots,0)$ 附近的邻域 $V=\{|t_i|<\epsilon, i=1,\cdots,r\}$ 内存在点 $(d_1,\cdots,d_r)$, 使得对于 $t_i=d_i+t_i', i=1,\cdots,r$, 集合 $\mathcal{P}$ 中的任何多项式当表示成为关于 t_i' 的多项式时, 不含任何 t_i' 的项不等于 0. 而且, V 中符合上述条件的点将形成一个开集且在 V 中是稠密的.

证明 对于 $\mathcal{P}$ 中每一个多项式 P, $\mathrm{Zero}_{\mathbf{R}}(P)$ 在 r 维实空间 $\mathbf{R}^r(t_1,\cdots,t_r)$ 中定义了一个拓扑维数至多为 $r-1$ 的实代数簇. 参见定理 5.1.45. 在原点 $(t_1,\cdots,t_r)=(0,\cdots,0)$ 的任意邻域中, 使得任何在集合 $\mathcal{P}$ 中的多项式都不为零的点 $(d_1,\cdots,d_r)$ 构成一个在 V 中稠密的开集. 在这个稠密开集中的任意点都满足我们的要求. □

定理 6.2.14 令 $c_i=c_{i0}+t_i$ 是给定的多项式集合 $PS\subset\mathbf{R}[x_1,\cdots,x_n]$ 的多项式的近似数值系数的某个准确表示, 其中精确度为 N. 那么对于足够小的 $\epsilon>0$, 有健康表示 $c_{i0}'+t_i'$, 其中基本部分为 c_{i0}', 微小部分为 t_i', 精确度为 N, 使得 $|c_{i0}'-c_{i0}|<\epsilon$.

证明 不失一般性, 我们假设给定的近似系数 $c_i=c_{i0}+t_i$ 的精确度为 $N'>N$. 如果这个近似不是健康的, 设 $\mathcal{P}$ 是所有关于 t_i 的形如 (6.2.27) 中的病态多项式 P_k' 的病态单项式的系数的多项式集合. 利用引理 6.2.13, 我们可以构造足够小的 $\epsilon>0$ 并且构造符合引理条件的邻域 $|t_i|<\epsilon$ 的点 $(d_1,\cdots,d_r)$. 那么, 准确表示 $c_i=c_{i0}'+t_i'$, 其中 $c_{i0}'=c_{i0}+d_i$, $t_i'=t_i-d_i$ 将是健康的, 精确度为 N, 满足我们的要求. □

注释 6.2.15 因为点 $(d_1,\cdots,d_r)$ 可以在 $\mathbf{R}^r(t_1,\cdots,t_r)$ 的原点的某个足够小的邻域的一个稠密开子集中任意选择, 几乎可以肯定, 随机选取这样的点 $(d_1,\cdots,d_r)$, 其中 d_i 足够小, 修改过的准确表示 $c_i=c_{i0}'+t_i'$, 其中 $c_{i0}'=c_{i0}+d_i, t_i'=t_i-d_i$ 将是健康的. 上面的定理 6.2.14 的确给出了实际中问题 H1 的一个解法.

<u>多变元多项式的近似因式分解</u>

我们现在来解决问题 H2. 对于符号计算方法, 多变元多项式的因式分解是不可避免的. 但是, 如果一个多项式的系数是近似数值, 那么很难断定给定

的多项式能不能分解. 例如, 多项式 $f = x^3 + y^3 + z^3 - 3.0 * x * y * z$ 中的系数 3.0 如果只是一个近似数值, 那么说 f 有一个因子 $g = x + y + z$ 是不合法的. 我们只能说 f 有近似因子 g. 这样的关于近似因式分解的概念已经在 Zassenhaus 的一些著作里出现, 而且, 最近它也出现在 Sasaki 等人的一些论文中, 可参看 [S-S-K-S]. 下面我们将用如下方法介绍近似因式分解的概念.

我们考虑一个准确表示的多项式 $f \in \mathbf{Q}[x, Y, t_1, \cdots, t_r]$, 这里 $Y = (y_1, \cdots, y_l)$ 是一个参数集, t_i 是微小部分也被看作参数. 首先, 我们考虑当基域是特征为 0 的一般域 $\mathbf{K}$, 而 Y 是不存在的情形.

定义 6.2.16 关于 x 的阶为 s 的多项式 $f \in \mathbf{K}[x, t_1, \cdots, t_r]$ 的近似因式分解是乘积

$$f = g * h \bmod T^{s+1}, \tag{6.2.28}$$

这里 g, h 是 $\mathbf{K}[x, t_1, \cdots, t_r]$ 上的关于 x 的次数为正整数的多项式, $\bmod T^{s+1}$ 意味着 (6.2.28) 对于阶大于 s 的微小部分是等式.

首先我们注意, 为了近似因式分解 f, 至多经过一个关于 x 和 t_i 的初等线性变换, 我们可以不失一般性假设

(S) 多项式 $f \in \mathbf{K}[x, t_1, \cdots, t_r]$ 关于 x 的首项系数不含任何 t_i.

在假设 (S) 下, 多项式 f 可以写成下面的形式:

$$f = f_0 + f_1 + \cdots + f_m, \tag{6.2.29}$$

这里对于每一个 j, f_j 关于变元 $t_1, \cdots, t_r$ 都是 j 次齐次的.

我们构造一个新的参数 u, 用 $u * t_i$ 替代每一个 t_i. 把多项式 $P \in \mathbf{K}[x, t_1, \cdots, t_r]$ 变换为多项式 $P^* \in \mathbf{K}[x, t_1, \cdots, t_r, u]$, 则 (6.2.29) 可以改写为

$$f^* = f_0 + u * f_1 + \cdots + u^m * f_m. \tag{6.2.30}$$

我们只要把 u 设为 1, 即可把 f^* 恢复成 f.

引理 6.2.17 因式分解 (6.2.28) 中的 f 等价于因式分解 f^*:

$$f^* = g^* * h^* \bmod u^{s+1}, \tag{6.2.31}$$

其中 g^*, h^* 是 $\mathbf{K}[x, t_1, \cdots, t_r, u]$ 中的多项式, 关于 x 的次数为正, 且 $\bmod u^{s+1}$ 是指等式 (6.2.31) 在相差一个关于 u 的次数大于 s 的因子时成立, 即 $f^* - g^* * h^*$ 是 u^{s+1} 的倍式.

证明 如果 (6.2.31) 是正确的, 那么设 $u = 1$ 我们将得到形如 (6.2.28) 中的 f 的近似因式分解, 其中多项式 $g, h \in \mathbf{K}[x, t_1, \cdots, t_r]$. 反之, 如果我们有形

如 (6.2.28) 中的 f 的近似因式分解, 其中多项式 $g, h \in \mathbf{K}[x, t_1, \cdots, t_r]$, 那么将每一个 t_i 用 $u * t_i$ 替换, 我们从 (6.2.28) 得到形如 (6.2.31) 的 f^* 的近似因式分解. □

如通常一样, 我们得到形如 (6.2.31) 的近似因式分解的方法是基于 [VdW2] 第 14 节中所示的 Hensel 构造.

定理 6.2.18 假设 (6.2.29) 中的 f_0 满足 (S), 并且 $\mathbf{K}[x]$ 中的 g_0, h_0 是已知的, 并且满足

$$f_0 = g_0 * h_0. \tag{6.2.32}$$

假设 f_0, g_0, h_0 关于 x 的次数分别是 n, p, q, 都为正, 且 $n = p + q$. 进一步假设 g_0, h_0 关于 x 有一个公因子 D. 那么对于给定的 s, 有算法可以判断 f 作为 $\mathbf{K}[x, t_1, \cdots, t_r]$ 中的一个多项式是否可以 s 阶近似因式分解, 当可以分解时, 给出形如 (6.2.28) 的近似因式分解. 如果 g_0, h_0 彼此互素, 这样的分解也存在, 并直接由算法给出近似因式分解.

证明 多项式 f_0, g_0, h_0 都在 $\mathbf{K}[x]$ 中. g, h 是 $\mathbf{K}[x, t_1, \cdots, t_r]$ 上要确定的多项式. 我们现在把 f^*, g^* 和 h^* 写成下面的形式:

$$\left.\begin{array}{rcl} f^* &=& f_0 + u * f_1 + \cdots + u^s * f_s \bmod u^{s+1}, \\ g^* &=& g_0 + u * g_1 + \cdots + u^s * g_s \bmod u^{s+1}, \\ h^* &=& h_0 + u * h_1 + \cdots + u^s * h_s \bmod u^{s+1}, \end{array}\right\} \tag{6.2.33}$$

这里对于每一个 k 所有 $\mathbf{K}[x, t_1, \cdots, t_r]$ 上的 f_k, g_k, h_k 对于 $t_1, \cdots, t_r$ 都是 k 次齐次的. 对于 $k = 1, 2, \cdots$, 我们的方法将由 f 和满足 (6.2.32) 的 g_0, h_0 来相继确定 g_k, h_k.

令 D 关于 x 的次数是 $d \geq 0$. 如果 g_0, h_0 彼此互素, 我们可以在后面令 $D = 1$ 且 $d = 0$. 我们有

$$g_0 = D * g_0', \; h_0 = D * h_0'.$$

类似地, g_0', h_0' 被看作 $\mathbf{K}[x]$ 上的多项式, 关于 x 的次数等于 $p' = p - d, q' = q - d$, 且彼此是互素的. 于是

$$\alpha * g_0' + \beta * h_0' = 1, \tag{6.2.34}$$

这里 $\alpha, \beta \in \mathbf{K}[x]$ 关于 x 的次数分别小于或等于 $q' - 1, p' - 1$.

现在，对于每一个 $k>0$ 且 $\leq s$ 我们暂时设

$$\left.\begin{aligned} F_k &= f_0+u*f_1+\cdots+u^k*f_k, \\ G_k &= g_0+u*g_1+\cdots+u^k*g_k, \\ H_k &= h_0+u*h_1+\cdots+u^k*h_k. \end{aligned}\right\} \tag{6.2.35}$$

这里 g_j,h_j 都是 $\mathbf{K}[x,t_1,\cdots,t_r]$ 上关于 $t_1,\cdots,t_r$ 是 j 次齐次的，且待定. 为了证明定理，对于 $k=1,2,\cdots,s$, 我们试图确定关于 x 的次数分别小于 p,q 的多项式 g_k,h_k; 且满足下面的等式:

$$F_k=G_k*H_k \bmod u^{k+1}. \tag{6.2.36}$$

为此，对每一个 $k>0$ 且 $\leq s$, 令

$$f_k^0=f_k-\sum_k g_i*h_j, \quad k\geq 1, \tag{6.2.37}$$

其中 $\sum_k$ 表示对所有满足 $i>0,j>0,i+j=k$ 的 (i,j) 求和. 因为 $f_0=g_0*h_0$, 所以方程组 (6.2.36) 等价于下面的一系列方程组:

$$g_0'*h_k+h_0'*g_k=\frac{f_k^0}{D},\ k\geq 1, \tag{6.2.38}$$

这里 f_k^0 由 (6.2.37) 给定. 我们将由 (6.2.38) 递归地确定 $g_k,h_k\in\mathbf{K}[x,t_1,\cdots,t_r]$. 很明显，如果 f_k^0 不能被 D 整除，那么将不存在这样的解 g_k,h_k, 从而问题中的近似因式分解是不可能的. 否则，$f_k'^0=\frac{f_k^0}{D}$ 是 $\mathbf{K}[x,t_1,\cdots,t_r]$ 上的一个多项式. 它关于 x 的次数小于 $n'=n-d=p+q'=p'+q$.

由 (6.2.34) 我们看到 (6.2.38) 有一个明显的解:

$$(g_k,h_k)=(\beta*f_k'^0,\alpha*f_k'^0). \tag{6.2.39}$$

但是多项式 g_k,h_k 关于 x 的次数太高而不能达到目的. 为了求得解 (g_k,h_k) 且次数分别小于或等于 $p-1,q-1$, 我们首先注意到 (6.2.38) 的每一个方程有如下形式:

$$g_0'*H+h_0'*G=F, \tag{6.2.40}$$

这里 g_0',h_0',F 是 $\mathbf{K}[x]$ 上关于 x 的次数分别等于 p',q' 且小于 n' 的已知的多项式，而 G,H 是 $\mathbf{K}[x]$ 上需要确定的关于 x 的次数分别小于 p',q' 的多项式. 因

为假设 (S), 我们可以将 g_0', h_0' 写成如下的形式 $(a_i, b_i \in \mathbf{K})$:

$$\left.\begin{aligned} g_0' &= a_{p'} * x^{p'} + \cdots + a_0, \\ h_0' &= b_{q'} * x^{q'} + \cdots + b_0. \end{aligned}\right\} \tag{6.2.41}$$

令 (6.2.40) 中的 F, G, H 由 $(e_i, c_i, d_i \in \mathbf{K}[t_1, \cdots, t_r])$ 分别表示成如下的形式:

$$\left.\begin{aligned} F &= e_{n'-1} * x^{n'-1} + \cdots + e_0, \\ G &= c_{p'-1} * x^{p'-1} + \cdots + c_0, \\ H &= d_{q'-1} * x^{q'-1} + \cdots + d_0, \end{aligned}\right\} \tag{6.2.42}$$

则 (6.2.40) 给出了一系列方程组

$$\sum_{i=1}^{r}(c_i * b_{r-i} + d_i * a_{r-i}) - e_r = 0, \tag{6.2.43}$$

其中 $r = 0, 1, \cdots, n' - 1$. 且对于 $i > p'$, $a_i = 0$, 对于 $i > q'$, $b_i = 0$, 对于 $i > p' - 1$, $c_i = 0$, 对于 $i > q' - 1$, $d_i = 0$.

设 M 是通常的关于两个多项式 g_0', h_0' 的 Sylvester 矩阵, 则 (6.2.43) 等价于下面的矩阵方程:

$$(d_{q'-1}, \cdots, d_0, c_{p'-1}, \cdots, c_0) * M = (e_{n'-1}, \cdots, e_0). \tag{6.2.44}$$

因为 g_0', h_0' 关于 x 没有公因子, 所以 M 的行列式是非零的, 因而元素在 $\mathbf{K}$ 上的逆矩阵 M^{-1} 是有明确定义的. 因此由 (6.2.44) 我们得到

$$(d_{q'-1}, \cdots, d_0, c_{p'-1}, \cdots, c_0) = (e_{n'-1}, \cdots, e_0) * M^{-1}. \tag{6.2.45}$$

用 $V_1, \cdots, V_n$ 表示 M^{-1} 的列向量, 用 E 表示向量 $(e_{n'-1}, \cdots, e_0)$. 我们得到下面关于 G 和 H 的显式表达式:

$$\left.\begin{aligned} G &= \sum_{p'} (E.V_{n'-i}) * x^i, \\ H &= \sum_{q'} (E.V_{q'-i}) * x^i, \end{aligned}\right\} \tag{6.2.46}$$

这里 $\sum_{p'}, \sum_{q'}$ 表示 i 分别从 0 到 $p'-1$ 和从 0 到 $q'-1$ 的求和. 很明显 (6.2.40) 中 (G, H) 的解是唯一的.

现在由 (6.2.38) 中 $k = 1$ 出发, 当 $k = 1, 2, \cdots, s$, 我们相继得到 (g_k, h_k), 由此 f_k^0 被 D 整除. 通过设 $u = 1$, 初始多项式 f 的相应的近似因子 g, h 将

会由 (6.2.33) 得到，但是 $g_k, h_k \in \mathbf{K}[x, t_1, \cdots, t_r]$. 如果在某个阶 k, 多项式 f_k^0 不能被 D 整除，则算法停止并且多项式 f 对于阶 $k \le s$ 不能被近似因式分解. □

<u>含参数多项式的近似因式分解</u>

现在考虑准确表示中包含参数 $Y = (y_1, \cdots, y_l)$ 的多项式 $f \in \mathbf{Q}[x, Y, t_1, \cdots, t_r]$ 的近似因式分解问题，其中微小部分 $(t_1, \cdots, t_r)$ 如前所述. 我们可以不失一般性的假设作为关于 x 的多项式 f 的首项系数不含 Y 和 $t_1, \cdots, t_r$. 如果需要，最多可以通过一个线性变换做到这一点. 让我们构造扩域 $\mathbf{K} = \mathbf{Q}(Y)$ 并认为 f 是 $\mathbf{K}[x, t_1, \cdots, t_r]$ 上的多项式. 那么 f 满足假设 (S), 同时定理 6.2.21 是适用的. 如果我们把 $\mathbf{K}$ 变回到 $\mathbf{Q}(Y)$ 并且把可能近似因式分解的多项式写成关于 $x, Y, t_1, \cdots, t_r$ 的有理函数的形式，那么将有一些关于 Y 的多项式单独出现在分母里. 去掉分数以后我们得到下面的定理作为定理 6.2.18 的一个推论:

定理 6.2.19 假设对于 (6.2.29) 中的 $f \in \mathbf{Q}[x, Y, t_1, \cdots, t_r]$, 每一个 f_k 在 $\mathbf{Q}[x, Y, t_1, \cdots, t_r]$ 上并且关于 $t_1, \cdots, t_r$ 是 k 次齐次的，其中 $f_0 \in \mathbf{Q}[x]$ 中不含 Y 和 $t_1, \cdots, t_r$. 假设 f_0 满足 (6.2.32), 其中 g_0, h_0 是 $\mathbf{Q}[x]$ 上的关于 x 的次数为正的已知的多项式，则存在某个算法用来判断是否存在多项式 $I, I_1, I_2 \in \mathbf{Q}[Y]$ 和多项式 $g, h \in \mathbf{Q}[x, Y, t_1, \cdots, t_r]$, 使得对于给定的 s, 我们有

$$I * f = g * h \bmod T^{s+1}, \tag{6.2.47}$$

这里 g, h 中不包含 $t_1, \cdots, t_r$ 的部分是 $I_1 * g_0, I_2 * h_0$ 与 $I_1 * I_2 = I$.

注释 6.2.20 在一个多项式集合 $PS \subset \mathbf{R}[X](X = (x_1, \cdots, x_n))$ 的特征列的计算过程中，利用上述定理我们把计算过程中可能遇到的某个多项式 f 近似因式分解. f 中的变量 x 将是一些 x_m, 而 Y 将是按自然序排序排在 x_m 前面的一部分变量 $x_1, \cdots, x_{m-1}$. 于是，(6.2.47) 中的多项式 I 可能被吸收到 f 的初式中. 从而使得进一步计算没有问题. 于是，定理 6.2.18 和 6.2.19 的确提供了问题 H2 的一个解法.

注释 6.2.21 近似因式分解的一些改进和混合计算方法的一些有趣的例子，可参见支丽红的博士论文 [Zhi].

<u>一些例子</u>

例 6.2.22 考虑多项式

$$f = x^3 + y^3 + z^3 - 3.0 * x * y * z,$$

其中 3.0 是一个近似数值系数. 对于 3.0 我们构造准确表达 $3+t$, 其中 t 是一个微小部分. 我们把 y, z 考虑成 Y, 从而力争把 f 近似分解成 2 阶. 应用定理 6.2.18, 6.2.19 证明中的符号, 我们看到

$$\begin{aligned}f_0 &= x^3 - 3*x*y*z + (y^3+z^3) = g_0 * h_0,\\ f_1 &= -t*x*y*z,\end{aligned}$$

其中

$$g_0 = x + (y+z),\ h_0 = x^2 - x*(y+z) + (y^2+z^2-y*z).$$

我们相继地得到

$$M = \begin{bmatrix} 1 & y+z & 0 \\ 0 & 1 & y+z \\ 1 & -(y+z) & y^2+z^2-y*z \end{bmatrix},$$

$$\text{Det } M = 3*(y^2+z^2+y*z),$$

$$M^{-1} = \begin{bmatrix} 2*(y^2+z^2)+y*z & (y+z)*(y^2+z^2-y*z) & (y+z)^2 \\ y+z & y^2+z^2-y*z & -(y+z) \\ -1 & 2*(y+z) & 1 \end{bmatrix} /\text{Det } M.$$

$$\begin{aligned}g_1 &= \frac{(y+z)*y*z*t}{\text{Det } M},\\ h_1 &= -\frac{(y+z)*y*z*t*x-(y^2+z^2-y*z)*y*z*t}{\text{Det } M}.\end{aligned}$$

$$g = g_0 + g_1,\ h = h_0 + h_1,$$

$$f = g*h \bmod t^2.$$

除去分母后, 我们最终得到需要的 f 的 2 阶近似因式分解. 近似因式分解方法也可以自然地用于准确的因式分解, 通过构造足够大的 s. 因此, 假设 (S) 的约束下, 它提供了另一种通常意义的多变元多项式的因式分解的方法.

例 6.2.23 我们再考虑例 4.5.16, 它来自于 [W-R], Ex. D17. 我们因式分解多项式:

$$\begin{aligned}f = x^4 &+ (-z+3)*x^3 + (z^3+(y-3)*z-y^2-13)*x^2\\ &+(-z^4+(y^2+3*y+15)*z+6)*x\\ &+y*z^4+2*z^3+(-y^3-15*y)*z-2*y^2-30.\end{aligned}$$

设

$$y = u*t_1, \quad z = u*t_2,$$

则 f 变成

$$f = f_0 + u * f_1 + \cdots + u^5 * f_5,$$

其中

$$\begin{aligned}
f_0 &= x^4 + 3 * x^3 - 13 * x^2 + 6 * x - 30, \\
f_1 &= x * t_2 * (-x^2 - 3 * x + 15), \\
f_2 &= t_1 * (x^2 * t_2 - x^2 * t_1 + 3 * x * t_2 - 15 * t_2 - 2 * t_1), \\
f_3 &= t_2 * (x^2 * t_2^2 + x * t_1^2 + 2 * t_2^2), \\
f_4 &= -t_2 * (x * t_2^3 + t_1^3), \\
f_5 &= t_2^4 * t_1.
\end{aligned}$$

我们有

$$f_0 = g_0 * h_0,$$

其中

$$g_0 = x^2 + 2,\ h_0 = x^2 + 3 * x - 15$$

是彼此互素的. 我们相继地得到:

$$\begin{aligned}
&\alpha = \frac{1}{307} * (3 * x + 26), \quad \beta = -\frac{1}{307} * (3 * x + 17), \\
&(g_1, h_1) = (-x * t_2, 0), \quad (g_2, h_2) = (t_2 * t_1, -t_1^2), \\
&(g_3, h_3) = (0, t_2^3), \quad (g_4, h_4) = (0, 0), \quad (g_5, h_5) = (0, 0). \\
&g = x^2 + 2 - u * x * t_2 + u^2 * t_2 * t_1, \\
&h = x^2 + 3 * x - 15 - u^2 * t_1^2 + u^3 * t_2^3.
\end{aligned}$$

由此, 我们发现 $f - g * h = 0$. 因此设 $u = 1, t_1 = y, t_2 = z$, 则 f 分解成

$$f = (x^2 - x * z + z * y + 2) * (x^2 + 3 * x + z^3 - y^2 - 15).$$

§6.3 求解计数几何中的问题

<u>一般计数几何的问题</u>

为了进一步说明我们的多项式方程组的求解算法, 让我们考虑计数几何中的问题. 计数几何问题是指:

问题 EG. 根据给定的几何约束, 找出满足给定的几何约束的几何体的个数.

一般来说, 可以通过引进合适的坐标系将满足要求的几何体用仿射空间 $\mathbf{K}^n(X)$ 中的点用 $X = (x_1, \cdots, x_n)$ 来表示, 其中 $\mathbf{K}$ 是一个特征为 0 的域,

X 满足一些多项式方程. 给定的几何约束通常也可以表示成以 X 为坐标和一些参数的多项式方程组. 在这里我们只考虑具有上述特点的计数几何问题. 因此, 我们可以将这类问题转化为多项式方程组的求解问题. 然后我们就可以用我们的方法来求解这个方程组.

作为代数几何的一章的经典计数几何

经典的计数几何构成了现代代数几何的一个非常吸引人的部分. 计数几何问题的求解是根据 §5.2 介绍的代数对应论中的计数原理. 用这种方法求解主要有以下一些限制.

第一, 几何体被限制在特征为 0 的代数闭域上的射影空间中的几何体, 主要是指复数域. 几何约束是指具有射影性质.

第二, 解的个数是指一般情况下的个数, 计数时要考虑重数的概念. 在非一般情况下, 并没有统一的办法来求解.

一个简单的例题: 平面中与三条直线相切的圆

我们的方法没有上述的限制. 几何体和几何约束可以是仿射的, 欧氏的, 射影的或者是其他类型, 只要它们在适当地坐标系下可以表示成多项式的形式就可以. 解的数量不再依赖于重数的概念, 而是用准确的方法求出的 (即不需要考虑重数). 而且考虑了所有可能的情况, 不论是一般的还是非一般的. 同时, 我们的方法不仅能给出解的数量, 而且能给出解的具体形式. 下面让我们来看一个例题:

例 6.3.1 确定一般平面上与三条给定的直线相切的圆的个数.

这个问题虽然非常简单, 但是却能很好地说明问题. 为了研究方便, 令其中一条给定的直线 L_0 作为 X 轴. 同时为了避免不必要的复杂, 让我们假设另外两条直线 L_1, L_2 都与 L_0 相交于不同的点, 我们将其中一个交点取作原点. 在坐标系 (X, Y) 中, 两条直线 L_1, L_2 可以用如下的方程来描述

$$\left.\begin{aligned} L_1:\ & X + v_1 * Y = 0, \\ L_2:\ & X + v_2 * Y - w_2 = 0,\ w_2 \neq 0. \end{aligned}\right\} \tag{6.3.48}$$

圆 Z 与直线 L_0 相切可以用下面的方程来表示:

$$Z : (X - x)^2 + (Y - y)^2 = y^2. \tag{6.3.49}$$

为了使得圆 Z 与直线 L_1, L_2 相切, 则必须有 $PS = 0$, $PS = \{P_1, P_2\}$, 其中

$$\left.\begin{aligned} P_1 &= (x + v_1 * y)^2 - (1 + v_1^2) * y^2, \\ P_2 &= (x + v_2 * y - w_2)^2 - (1 + v_2^2) * y^2. \end{aligned}\right\} \tag{6.3.50}$$

我们取定变量的序为 $y \prec x$, 则特征集是 $CS = \{C_1, C_2\}$, 其中

$$\left.\begin{aligned} C_1 &= 4*y^4*(v_2-v_1)^2 - 8*y^3*w_2*(v_2-v_1)*(v_1*v_2+1)\\ &\quad -4*y^2*w_2^2*((v_2-v_1)^2-(v_2*v_1+1))\\ &\quad +4*y*w_2^3*(v_2-v_1)-w_2^4,\\ C_2 &= 2*x*(y*(v_2-v_1)-w_2)-2*y*w_2*v_2+w_2^2. \end{aligned}\right\} \quad (6.3.51)$$

由整序原理，我们有

$$\left.\begin{aligned} &\mathrm{Zero}(PS\ /\ w_2)\\ =&\ \mathrm{Zero}(CS\ /\ (v_2-v_1)*(y*(v_2-v_1)-w_2)*w_2)\\ &+\mathrm{Zero}(PS+\{v_2-v_1\}\ /\ w_2)\\ &+\mathrm{Zero}(PS+\{y*(v_2-v_1)-w_2\}\ /\ (v_2-v_1)*w_2). \end{aligned}\right\} \quad (6.3.52)$$

很容易证明除非 $v_2 = -v_1$, 否则最后一个零点集是空集. 于是我们只需要考虑三种情况 $v_2^2 \neq v_1^2, v_2 = v_1$, 或 $v_2 = -v_1 \neq 0$. 这三种情况中的零点集的并是 $\mathrm{Zero}(PS\ /\ w_2)$, 它们分别是如下的形式:

$$\left.\begin{aligned} &\mathrm{Zero}(CS\ /\ w_2)\ \text{当}v_2^2 \neq v_1^2,\ v_1, v_2 \neq 0\text{时},\\ &\mathrm{Zero}(CS^1\ /\ w_2)\ \text{当}\ v_2 = v_1 \neq 0\text{时},\\ &\mathrm{Zero}(CS^2\ /\ w_2)+\mathrm{Zero}(CS^3\ /\ w_2),\ \text{当}\ v_2 = -v_1 \neq 0\text{时}. \end{aligned}\right\} \quad (6.3.53)$$

特征集 $CS^i = \{C_1^i, C_2^i\}(i = 1, 2, 3)$ 分别是

$$\left.\begin{aligned} C_1^1 &= 4*y^2*(v_1^2+1)-w_2^2,\\ C_2^1 &= 2*x+2*y*v_1-w_2. \end{aligned}\right\} \quad (6.3.54)$$

$$\left.\begin{aligned} C_1^2 &= 2*v_1*y+w_2,\\ C_2^2 &= 4*v_1^2*x^2-4*v_1^2*w_2*x-w_2^2. \end{aligned}\right\} \quad (6.3.55)$$

$$\left.\begin{aligned} C_1^3 &= 4*y^2-4*v_1*w_1*y-w_2^2,\\ C_2^3 &= 2*x-w_2. \end{aligned}\right\} \quad (6.3.56)$$

不同的零点集的几何意义是非常明显的. (6.3.53) 中的第一个表达式和第三个表达式说明在一般情况下, 即给定的三条直线能够形成一个正确的三角形, 有四个圆与给定的三条直线相切, 分别对应着三角形的内切圆和外切圆. 当给定的三条直线是实的时候, 很容易验证四个与这三条直线相切的圆也是实的. 另一方面, (6.3.53) 中的第二个表达式说明当 L_1, L_2 平行但不相等, 并且与 L_0 相交于两个不同的点的时候, 只有两个圆和这三条直线相切.

进一步的示例：Appolonius 问题和 Malfatti 问题

让我用两个经典的问题来进一步说明我们的方法的求解过程.

Appolonius 问题 A. 确定普通平面上与三个给定的圆相切的圆的个数.

Malfatti 问题 M. 给定普通平面上一个三角形，确定与这个三角形中其中的两条边相切并且彼此互相相切的三个圆所构成的三元组的个数.

在求解这两个问题之前，首先让我们给出几点说明.

在一个实的普通平面上，一条直线或者一个圆将会将整个平面分成两个部分. 当一个圆与一条直线相切时，这个圆或者在直线的这边或者在另一边. 同理，两个圆互相相切时，或者外切或者内切. 但是，当在特征为 0 的非实的域即复数域中，则上面讲过的概念就没有什么意义了. 在实平面的情况下，我们将直线或者圆与圆相切的两种的情况，看作两种不同的情况. 为此我们引进有向直线和有向圆的概念.

有向直线的定向坐标

下面我们考虑域 $\mathbf{R}$ 上的一般平面，用 (X,Y) 作为运动的坐标.

定义 6.3.2 直线

$$L:\ u*X+v*Y=w,\ \ L':\ u'*X+v'*Y=w'$$

称为是正等价的是指存在一个非零的元素 $k\in\mathbf{R}$, 使得

$$u'=k^2*u,\ v'=k^2*v,\ w'=k^2*w.$$

定义 6.3.3 我们将所有直线在正等价关系下的一个等价类称为一条有向直线.

注释 6.3.4 为了不引起混淆，我们认为一条有向直线与其所在等价类中其他的直线看成是等价的.

定义 6.3.5 我们将有向直线 $-u*X-v*Y=-w$ 称为有向直线 $u*X+v*Y=w$ 的反向直线.

记号 6.3.6 分别将有向直线 $+L$ 和 $-L$ 的反向直线记为 $-L$ 和 $+L$.

定义 6.3.7 我们将 $(u:v:w)^+$ 称为有向直线 $+L: u*X+v*Y=w$ 的定向坐标.

定义 6.3.8 我们将有向直线等价类中的一条有向直线 $u*X+v*Y=w$, $u^2+v^2=1$ 称为有向直线的规范形式.

定义 6.3.9 我们将有向直线等价类中的具有规范形式的有向直线的定向坐标称为有向直线的正规化坐标.

注释 6.3.10 让我们用一个例子来更好地说明上面给出的定义. 有向正

直线 X 轴可以用 $+Y=0$ 来表示，它的正规化坐标是 $(0:1:0)^+$. 有向直线 Y 轴的反向直线是 $-Y=0$, 它的正规化坐标是 $(0:-1:0)^+$.

有向圆的定向坐标

任意一个以 (x,y) 为圆心，以 $|r|\geq 0$ 为半径的实平面上的圆都可以表示成如下的形式:

$$(X-a)^2+(Y-b)^2=r^2. \tag{6.3.57}$$

当 $r\neq 0$ 时，根据 r^2 中的 r 的取值不同, $+r$ 或者 $-r$, 我们将上式看成两个有向圆.

定义 6.3.11 我们用三元组 (a,b,r) 和 $(a,b,-r)$ 表示与表达式 (6.3.57) 对应的两个具有相反方向的有向圆.

定义 6.3.12 我们将有向圆 (a,b,r) 的半径 r 称为有向圆的有向半径.

记号 6.3.13 与有向圆 $+Z$ (或者 $-Z$) 具有相反方向的有向圆记为 $-Z$ (或者 $+Z$).

注释 6.3.14 我们可以很自然地把有向圆和有向直线的概念推广到普通的实空间上，从而定义有向平面和有向球.

有向直线和有向圆的定向相切

定义 6.3.15 一条具有正规化坐标 (u,v,w) 的有向直线在同向的意义下 (或者在反向的意义下) 与有向圆 (x,y,r) 相切是指

$$\left.\begin{aligned} &u*x+v*y=w+r, \\ \text{或者}\quad &\\ &u*x+v*y=w-r. \end{aligned}\right\} \tag{6.3.58}$$

定义 6.3.16 我们将满足

$$\left.\begin{aligned} &(x_1-x_2)^2+(y_1-y_2)^2=(r_1-r_2)^2, \\ \text{或者}\quad &\\ &(x_1-x_2)^2+(y_1-y_2)^2=(r_1+r_2)^2 \end{aligned}\right\} \tag{6.3.59}$$

的两个有向圆 $(x_1,y_1,r_1),(x_2,y_2,r_2)$ 称为是在同向的意义下 (或者是反向意义下) 相切的.

注释 6.3.17 我们可以用一个简单的例子来说明这一点，例如，有向圆 (x,y,y) 与正向 X 轴 $+Y=0$ 在同向的意义下是相切的.

求解 Appolonius 问题

例 6.3.18 (Appolonius 问题 A) 对于 $i=1,2,3$, 令 Z_i 是三个具有有向坐标 (a_i,b_i,c_i) 的有向圆, Z 是具有有向坐标 (x,y,r) 的想要求的有向圆. 让我们

用 e_i, $e_i^2=1$ 来表示有向圆 Z 和 Z_i 相切，则 Z 和 Z_i 相切可以用下面的式子来表示：

$$P_i \equiv (x-a_i)^2+(y-b_i)^2-(r-e_i*c_i)^2=0,\ i=1,2,3. \tag{6.3.60}$$

把 a_i,b_i,c_i,e_i 看作是常量参数，变量 r,x,y 的序是 $r \prec x \prec y$, $PS=\{P_1,P_2,P_3\}$ 特征集是 $CS=\{C_1,C_2,C_3\}$, 其中 C_i 的指标集是

$$[593\ r\ 2],\ [30\ x\ 1],\ [30\ y\ 1]. \tag{6.3.61}$$

让我们只考虑一下一般的情况，即 C_i 的初式都是非零的. 对于每一个取定固定值的三元组的 $(e_1,e_2,e_3)=(\pm1,\pm1,\pm1)$ 集合，将会有两个有向圆与给定的三个有向圆相切. 根据相切的方式不同，Appolonius 问题 A 有 16 个解. 但是，当四元组 (r,e_1,e_2,e_3) 变成 $(-r,-e_1,-e_2,-e_3)$ 时，C_1 依然是不变的，因此 Appolonius 问题解的数量将是 8. 而且，因为关于 r 的方程的次数是 2, 所以可能有复数解. 在此，我们不考虑几何实现的问题和实解的准确数目，它们在每种具体情况下都可以精确求出来.

Malfatti 问题的求解

例 6.3.19 (Malfatti 问题 M) 令三角形是 $A_1A_2A_3$, 三个要求的圆 Z_i 的圆心是 O_i, $i=1,2,3$. 很明显，A_1O_1,A_2O_2,A_3O_3 分别是三角形的三个角的角平分线. 根据三个角平分线是否交于一点，可以将问题分成两种情况来考虑. 首先让我们来考虑三条角平分线，则交于一点 I, I 是内心或者是三角形的三个外心中的任意一个.

让我们取定坐标系使得

$$A_1=(a_1,0),\ A_2=(a_2,0),\ I=(0,c), \tag{6.3.62}$$

则顶点 A_3 的坐标是

$$A_3=(a_3,b_3), \tag{6.3.63}$$

其中

$$a_3=\frac{c^2*(a_1+a_2)}{c^2+a_1*a_2},\quad b_3=\frac{2*c*a_1*a_2}{c^2+a_1*a_2}. \tag{6.3.64}$$

令圆 Z_i 的圆心的坐标是 (x_i,y_i), $i=1,2,3$, 则 x_i,y_i 满足方程 $P_i=0$, $i=1,2,3$, 其中

$$\left.\begin{aligned}
&P_1=y_1*a_1+x_1*c-c*a_1;\\
&P_2=y_2*a_2+x_2*c-c*a_2;\\
&P_3=y_3*c*(a_2+a_1)+x_3*(c^2-a_2*a_1)-c^2*(a_2+a_1).
\end{aligned}\right\} \tag{6.3.65}$$

另一方面，圆 Z_i 的半径分别是 $|y_1|,|y_2|,|r_3|$，则有下面的等式成立：

$$r_3 = \frac{c*(a_3 - x_3)}{a_3} = \frac{c*(b_3 - y_3)}{b_3 - c}. \tag{6.3.66}$$

现在让我们将圆 Z_i 进行定向，使得有向圆 $+Z_i$ 用下面的有向坐标来表示：

$$+Z_1 = (x_1, y_1, +y_1), \quad +Z_2 = (x_2, y_2, +y_2), \quad +Z_3 = (x_3, y_3, +r_3). \tag{6.3.67}$$

我们将圆 $Z_i(i = 1,2,3)$ 彼此互相相切用方程 $P_j = 0(j = 4,5,6)$ 来表示，其中，

$$\left.\begin{aligned}
P_4 &= 2*y_2*y_1*(e_3-1)+(x_2-x_1)^2;\\
P_5 &= -4*y_3^2*c^2*a_2*a_1\\
&\quad +2*y_3*y_1*e_2*(c^4-a_2^2*a_1^2)-2*y_3*y_1*(c^2-a_2*a_1)^2\\
&\quad +4*y_3*c*a_2*a_1*(c^2+a_2*a_1)\\
&\quad -4*y_1*e_2*c*a_1*a_2*(c^2-a_2*a_1)^2\\
&\quad +(x_3-x_1)^2*(c^2-a_2*a_1)^2-4*c^2*a_2^2*a_1^2;\\
P_6 &= -4*y_3^2*c^2*a_2*a_1\\
&\quad +2*y_3*y_2*e_1*(c^4-a_2^2*a_1^2)-2*y_3*y_2*(c^2-a_2*a_1)^2\\
&\quad +4*y_3*c*a_2*a_1*(c^2+a_2*a_1)\\
&\quad -4*y_2*e_1*c*a_1*a_2*(c^2-a_2*a_1)^2\\
&\quad +(x_3-x_2)^2*(c^2-a_2*a_1)^2-4*c^2*a_2^2*a_1^2.
\end{aligned}\right\} \tag{6.3.68}$$

在方程组 (6.3.68) 中，我们引进 $e_i(e_i^2 = 1,\ i = 1,2,3)$ 来表示圆之间的不同的相切方式. 令变量的序是

$$x_1 \prec x_2 \prec x_3 \prec y_1 \prec y_2 \prec y_3. \tag{6.3.69}$$

令 $PS = \{P_1, \cdots, P_6\}$. 我们用符号 $\text{Zero}^{(+-+)}$ 记零点集 $e_1 = +1, e_2 = -1, e_3 = +1$. 则软件包 wsolve 很容易地给出如下的结果：

$$\left.\begin{aligned}
&\text{Zero}^{(s)}(PS) = \text{Zero}(CS^{(s)}/IP^{(s)}),\\
&\qquad\qquad \text{当 } (s) = (+++),(++-),(+-+),(-++),\\
&\text{Zero}^{(s)}(PS) = \textstyle\bigcup_{k=1,2}\ \text{Zero}(CS_k^{(s)}/IP_k^{(s)}),\\
&\qquad\qquad \text{当 } (s) = (+--),(-+-),(--+),(---).
\end{aligned}\right\} \tag{6.3.70}$$

在式 (6.3.70) 中，我们用 IP 表示相应的初式积. 对于 $(s) = (+++)$，相应的特征集是 $CS^{(+++)} = \{x_1, x_2, x_3, y_1 - c, y_2 - c, y_3 - c\}$，这表明三个圆 Z_i 将退化成以一个 I 为圆心的三角形的内切圆或者是外接圆.

对于 (s) = $(---)$ 或者 $(+++)$, 问题的解也有明显的几何意义. 例如, (s)=$(-++)$ 时, x_1=x_2, 这表明圆 Z_1, Z_2 互相相切并且与 X 轴切于同一点.

对于 $(s) = (---)$, 相应的特征集 $CS_1^{(s)}$ 和 $CS_2^{(s)}$ 具有以下指标集的多项式:

$$[49\ x_1\ 4],\ [78\ x_2\ 1],\ [212\ x_3\ 1],\ [3\ y_1\ 1],\ [76\ y_2\ 1],\ [200\ y_3\ 1]. \tag{6.3.71}$$

因此, 对于 (s) 的这种情况, 对于给定的内心后者外心 I, 我们得到 8 个解. 由于对 I 有四种选择, 因此我们可以得到 32 个解. Steiner 在 [St], [Pet] 中给出了一般的解.

三个角平分线不共点的情况可以用相同的方法来处理, 所有的解, 无论是平凡的, 还是一般的都可以被完全确定. 注意到, 这种情形似乎被 Steiner 和其他研究这个问题的几何专家所忽略. 在此, 我们没有考虑实现的条件.

<u>射影空间中三次曲面上的直线</u>

我们用方程 $S = 0$ 来描述射影空间 $P^3_{\mathbf{K}}(Z)(Z = (z_0 : z_1 : z_2 : z_3))$ 中的一个三次曲面 S_3, 其中,

$$\left.\begin{aligned} S = {} & a_1 * z_0^3 + a_2 * z_1^3 + a_3 * z_2^3 + a_4 * z_3^3 \\ & + a_5 * z_0^2 * z_1 + a_6 * z_0^2 * z_2 + a_7 * z_0^2 * z_3 \\ & + a_8 * z_0 * z_1^2 + a_9 * z_1^2 * z_2 + a_{10} * z_1^2 * z_3 \\ & + a_{11} * z_0 * z_2^2 + a_{12} * z_1 * z_2^2 + a_{13} * z_2^2 * z_3 \\ & + a_{14} * z_0 * z_3^2 + a_{15} * z_1 * z_3^2 + a_{16} * z_2 * z_3^2 \\ & + a_{17} * z_0 * z_1 * z_2 + a_{18} * z_0 * z_1 * z_3 \\ & + a_{19} * z_0 * z_2 * z_3 + a_{20} * z_1 * z_2 * z_3. \end{aligned}\right\} \tag{6.3.72}$$

例 6.3.20 问题: 假设三次曲面 S_3 上包含有有限条直线, 确定三次曲面 S_3 上所包含的直线的条数.

根据代数对应理论中的计数原理, 我们可以知道如果一个三次曲面上的直线的条数不是无限的, 那么在考虑重数的情况下, 一般是 27 条, 参见 [VdW2]. 在这里, 我们将用我们的方法来精确地求出一个一般的三次曲面上的直线的个数 (不考虑重数), 并且可以求出这些直线本身.

为了讨论方便, 我们假设三次曲面 S_3 不是一个锥面, 同时也不包含一个平面, 否则这个三次曲面将包含有无穷条直线. 我们将按照下面的方法取定一个四面体的坐标系 $U_0U_1U_2U_3$. 首先, 我们在 S_3 上取一个点 U_3, 使得在点 U_3 的切平面 T_3 与 S_3 交于一条非退化的三次曲线 C_3. 然后, 我们在 C_3 上取一

点 U_2, 使得在点 U_2 的切平面 T_2 不同于 T_3, 同时 T_2 与 C_3 交于一个不同于点 U_2 的 U_1 点，则在点 U_1 的切平面 T_1 既不包含点 U_2 也不包含点 U_3, 否则直线 U_1U_2(或者 U_1U_3) 将会与三次曲面 S_3 交于四个点，两个在点 U_1, 另外两个在点 U_2 (或者 U_3), 但是这是不可能的. 于是，点 U_1 处的切平面 T_1 将与 T_2 交于一条直线，这条直线与三次曲面 S_3 交于三个点，其中两个在点 U_1, 我们将第三个点记为 U_0.

从上面的坐标系的取法中，我们可以看出 T_3 就是平面 $U_1U_2U_3$, T_2 就是平面 $U_0U_1U_2$, T_1 包含直线 U_0U_1. 这些分别等价于下面的等式:

$$a_{15} = a_{16} = 0,\ a_{11} = a_{12} = 0,\ a_8 = 0. \tag{6.3.73}$$

现在我们考虑任意一条直线 L, 其 Pluecker 坐标是 $(p_{01} : p_{02} : p_{03} : p_{12} : p_{13} : p_{23})$. 直线 L 如果不在任意一个坐标平面 $z_i = 0 (i = 0, 1, 2, 3)$ 上，则与这些坐标平面交于点 $P_0 = (0 : p_{01} : p_{02} : p_{03})$, $P_1 = (-p_{01} : 0 : p_{12} : p_{13})$, $P_2 = (-p_{02} : -p_{12} : 0 : p_{23})$, $P_3 = (-p_{03} : -p_{13} : -p_{23} : 0)$. 我们首先假设直线 L 完全在三次曲面 S_3 上. 由上面的构造，直线 U_2U_3 不在 S_3 上，因此 $p_{01} \neq 0$, 则直线 L 在 S_3 上当且仅当对任意的 u, 点 $Q_u = P_0 + u * P_1$ 在 S_3 上. 由此我们可以得到直线完全在 L 的充分必要条件是 $P_{ui} = 0, i = 0, 1, 2, 3$, 其中多项式 P_{ui} 由下式给出:

$$\left.\begin{aligned}
P_{u0} = {} & p_{03} * p_{02}^2 * a_{13} + p_{03} * p_{02} * p_{01} * a_{20} \\
& + p_{03} * p_{01}^2 * a_{10} + p_{02} * p_{01}^2 * a_9, \\
P_{u1} = {} & p_{13} * p_{02}^2 * a_{13} + p_{13} * p_{02} * p_{01} * a_{20} \\
& + p_{13} * p_{01}^2 * a_{10} + 2 * p_{12} * p_{03} * p_{02} * a_{13} \\
& + p_{12} * p_{03} * p_{01} * a_{20} + p_{12} * p_{01}^2 * a_9 \\
& - p_{03}^2 * p_{01} * a_{14} - p_{03} * p_{02} * p_{01} * a_{19} \\
& - p_{03} * p_{01}^2 * a_{18} - p_{02} * p_{01}^2 * a_{17}, \\
P_{u2} = {} & 2 * p_{13} * p_{12} * p_{02} * a_{13} + p_{13} * p_{12} * p_{01} * a_{20} \\
& - 2 * p_{13} * p_{03} * p_{01} * a_{14} - p_{13} * p_{02} * p_{01} * a_{19} \\
& - p_{13} * p_{01}^2 * a_{18} + p_{12}^2 * p_{03} * a_{13} \\
& - p_{12} * p_{03} * p_{01} * a_{19} - p_{12} * p_{01}^2 * a_{17} \\
& + p_{03} * p_{01}^2 * a_7 + p_{02} * p_{01}^2 * a_6 + p_{01}^3 * a_5, \\
P_{u3} = {} & - p_{13}^2 * p_{01} * a_{14} + p_{13} * p_{12}^2 * a_{13} \\
& - p_{13} * p_{12} * p_{01} * a_{19} + p_{13} * p_{01}^2 * a_7 \\
& + p_{12} * p_{01}^2 * a_6.
\end{aligned}\right\} \tag{6.3.74}$$

另外，我们还知道 $PL=0$, 其中

$$PL = p_{23} * p_{01} - p_{13} * p_{02} + p_{12} * p_{03}, \tag{6.3.75}$$

则我们可以得到一个多项式集 $PS = \{P_{u0}, P_{u1}, P_{u2}, P_{u3}, PL\}$, 三次曲面 S_3 上的直线可以由零点集 Zero(PS) 给出. 令变量 $p_{ij}(i<j)$ 的序是

$$p_{01} \prec p_{02} \prec p_{03} \prec p_{12} \prec p_{13} \prec p_{23},$$

则特征集 CS 将包含五个多项式 C_i, $i=1,\cdots,5$, 其中 C_1 是不可约的，索引集如下：

$$[15895\ p_{02}\ 27],\ [4\ p_{03}\ 1],\ [1245\ p_{12}\ 1],\ [10\ p_{13}\ 1],\ [3\ p_{23}\ 1].$$

初式是 $I_i, i=1,\cdots,5$, 其中

$$I_1 = a_5^2 * a_6 * a_9 * a_{13} * a_{15}.$$

由此我们可以得知，对于一般情况， $I_i \neq 0$, $i=1,\cdots,5$ 和 C_1 关于 p_{02} 的判别式不等于零，三次曲面 S_3 上的直线的条数将是 27, 并且直线方程可以由零点集 Zero(PS) 给出. 对于非退化的情况，只要令某些初式和 (或者)C_1 的判别式为零，我们也可以用类似的方法进行处理.

§6.4 星体运动与涡流运动的中心构型

天体力学中的中心构型

记号 6.4.1 $J_n = \{1,\cdots,n\}$;

$J_n^2 = \{(i,j) \mid i,j \in J_n, i \neq j\}$;

用 $m_1,\cdots,m_n$ 代表处于相互牛顿引力作用下运动的 n 粒子的质量.

用 $\mathbf{r}_1,\cdots,\mathbf{r}_n$ 代表这些质量在某一时刻的位置，其中 $\mathbf{r}_i \neq \mathbf{r}_j$ 当$i \neq j$.

用 $\begin{bmatrix} m_1 & m_2 & \cdots & m_n \\ \mathbf{r}_1 & \mathbf{r}_2 & \cdots & \mathbf{r}_n \end{bmatrix}$ 代表一个 构型, 它由在某一位置 $\mathbf{r}_i(i \in J_n)$ 的 m_i 形成.

定义 6.4.2 相对于质量 $m_1,\cdots,m_n$ 的构型

$$\begin{bmatrix} m_1 & m_2 & \cdots & m_n \\ \mathbf{r}_1 & \mathbf{r}_2 & \cdots & \mathbf{r}_n \end{bmatrix}$$

是一个 刚体构型 (中心构型) 当且仅当质量 m_i 具有初速度，使得处于牛顿引力作用下时，由某一时刻的质量形成的构型相对与初始构型保持 相同 (或 相似).

对于刚体或中心构型 $\begin{bmatrix} m_1 & m_2 & \cdots & m_n \\ \mathbf{r}_1 & \mathbf{r}_2 & \cdots & \mathbf{r}_n \end{bmatrix}$ 牛顿力学的一个直接结果是：这些质量 $m_1,\cdots,m_n$ 所形成的物体的中心在某一时刻的位置可以认为是固定的.

定义 6.4.3　伴随刚体或中心构型 $\begin{bmatrix} m_1 & m_2 & \cdots & m_n \\ \mathbf{r}_1 & \mathbf{r}_2 & \cdots & \mathbf{r}_n \end{bmatrix}$ 的*惯性坐标系*是指笛卡儿坐标系，原点在质量 $m_1,\cdots,m_n$ 所形成的物体的固定中心的位置.

作为牛顿力学的另一个直接结果，我们有下面的命题：

命题 6.4.4　对于刚体或中心构型 $\begin{bmatrix} m_1 & m_2 & \cdots & m_n \\ \mathbf{r}_1 & \mathbf{r}_2 & \cdots & \mathbf{r}_n \end{bmatrix}$ 在任意伴随的惯性坐标系中，我们都有

$$\sum_i m_i * \mathbf{r}_i = 0. \tag{6.4.76}$$

定义 6.4.5　两个相对于相同质量 $m_1,\cdots,m_n$ 的刚体构型属于相同的*构型类*当且仅当它们具有相同的质量中心，而且存在一个保持方向的相似变换，它使得质量中心保持不变，同时将一个构型转化成另一个.

<u>关于中心构型的历史注记</u>

显然刚体构型也是一个与其具有相同质量集的中心构型. 反之也是正确的，这里我们省略证明. 见 [Wint] 中的例子. 因此我们有结论：一个中心构型决定了一类刚体构型，反之亦然.

下面我们只考虑惯性坐标系.

记号 6.4.6　用 $q_3(n) = q_3(n; m_1,\cdots,m_n)$ 代表给定质量 $m_1,\cdots,m_n$ 的刚体构型的类的个数.

用 $q_2(n) = q_2(n; m_1,\cdots,m_n)$ 代表给定质量 $m_1,\cdots,m_n$ 刚体构型的类的个数，其中这些质量 m_i 在同一平面上.

用 $q_1(n) = q_1(n; m_1,\cdots,m_n)$ 代表给定质量 $m_1,\cdots,m_n$ 刚体构型的类的个数，其中这些质量 m_i 在同一条线上.

注释 6.4.7　我们的记号与 Wintner 在其书 [Wint] 中的那些不同，因为 Wintner 书中的 q_2, q_3 对应于这里的 $q_2 - q_1, q_3 - q_2$.

已知的结果. 对于给定的质量 $m_1,\cdots,m_n$,

我们有

$q_1(2) = q_2(2) = q_3(2) = 1$;

$q_1(3) = 3$ (Euler 1767);

$q_2(3) = q_3(3) = 5$ (Lagrange 1772);

$q_1(n) = \frac{n!}{2}$ (Moulton 1910, [Mou]);

$q_3(n) > q_2(n)$, 其中 $n > 4$, 由 $m_1, \cdots, m_n$ 形成的某些特殊集合 (Waldvogel 1972, [Wald]).

显然

$$q_1(n; m_1, \cdots, m_n) \leq q_2(n; m_1, \cdots, m_n) \leq q_3(n; m_1, \cdots, m_n). \tag{6.4.76'}$$

由 Moulton 的结果，我们有 $q_1(n; m_1, \cdots, m_n)$ 是有限的，对于所有的 n 和质量 $m_1, \cdots, m_n$.

Wintner 猜想. 对于所有的 n 和质量 $m_1, \cdots, m_n$, $q_3(n; m_1, \cdots, m_n)$ 和 $q_2(n; m_1, \cdots, m_n)$ 都是有限的.

近几年来 Smale 和他的同事们利用拓扑学方法中的 Morse 临界点理论研究了中心构型. 见例如 [Sm1,2]. Wintner 的猜想似乎仍未解决. 本节中，我们只限于研究刚体与中心构型的实际确定，并把它作为多项式求解来处理. 为此，我们将采用伴随刚体或中心构型 $\begin{bmatrix} m_1 & m_2 & \cdots & m_n \\ \mathbf{r}_1 & \mathbf{r}_2 & \cdots & \mathbf{r}_n \end{bmatrix}$ 的惯性坐标系.

我们将用到下列记号:

记号 6.4.8

$$\mathbf{r}_i = (x_i, y_i),\ i \in J_n;$$
$$x_{ij} = x_i - x_j,\ y_{ij} = y_i - y_j,\ (i,j) \in J_n^2;$$
$$r_{ij} = \sqrt{x_{ij}^2 + y_{ij}^2},\ (i,j) \in J_n^2.$$

<u>刚体构型的基本方程</u>

对于平面上的一个刚体构型 $\begin{bmatrix} m_1 & m_2 & \cdots & m_n \\ \mathbf{r}_1 & \mathbf{r}_2 & \cdots & \mathbf{r}_n \end{bmatrix}$, 我们知道在运动过程中，平面是固定的，这样就能使中心构型与原始的保持一致. 现在我们取平面惯性坐标系 (x, y), 坐标原点 O 在质量中心，则中心构型就会以一定的角速度围绕 O 运动，并使得

$$\left.\begin{aligned} \omega^2 * x_i = \sum_{j \neq i} m_j * \frac{x_{ij}}{r_{ij}^3}, \\ \omega^2 * y_i = \sum_{j \neq i} m_j * \frac{y_{ij}}{r_{ij}^3}, \end{aligned} \quad i \in J_n. \right\} \tag{6.4.77}$$

式子右边表示所有其他质量作用于 m_i 的牛顿引力 (可能相差一个非零常数因子), 而式子的左边表示相应的离心力. 特别地，(6.4.77) 中所有方程中的 ω 是一个常量. 进而，当原点保持不动时，在进行保方向的相似变换时，这些方程

都保持不变但是常量 ω 可能发生变化.

我们假设 $r_{ij} \neq 0, (i,j) \in J_n^2$, 这意味着碰撞不予考虑. 因此刚体构型与中心构型的决定性因素就归结到求 (6.4.77) 中的方程组的解. 首先我们要去掉方程中的分母. 为了求解容易, 我们将引入关于 (6.4.77) 的一些基本变换, 使得求解更简单.

我们取复数域 $\mathbf{C}$ 为基本域, 而且引入复变量 u_i, v_i, z_{ij}, w_{ij} 如下 ($\mathbf{i}$ 表示 $\sqrt{-1}$):

$$\left.\begin{aligned} &u_i = x_i + \mathbf{i} * y_i,\ v_i = x_i - \mathbf{i} * y_i,\ i \in J_n, \\ &z_{ij} = \frac{1}{(u_i - u_j) * r_{ij}},\ w_{ij} = \frac{1}{(v_i - v_j) * r_{ij}},\ (i,j) \in J_n^2, \\ &\quad m_0 = -\ \omega^2. \end{aligned}\right\} \tag{6.4.78}$$

由 (6.4.77), 我们有下面的多项式方程组:

$$\left.\begin{aligned} &m_0 * u_i + \sum_{j \neq i} m_j * w_{ij} = 0, \\ &m_0 * v_i + \sum_{j \neq i} m_j * z_{ij} = 0, \end{aligned}\quad i \in J_n,\right\} \tag{6.4.79}$$

$$\left.\begin{aligned} &(u_i - u_j) * z_{ij} * r_{ij} - 1 = 0, \\ &(v_i - v_j) * w_{ij} * r_{ij} - 1 = 0, \\ &r_{ij}^2 - (u_i - u_j) * (v_i - v_j) = 0, \end{aligned}\quad (i,j) \in J_n^2.\right\} \tag{6.4.80}$$

$$r_{ij} - r_{ji} = 0,\ z_{ij} + z_{ji} = 0,\ w_{ij} + w_{ji} = 0,\ \ (i,j) \in J_n^2. \tag{6.4.81}$$

对于这些方程, 我们可以添加由 (6.4.76) 或 (6.4.77) 所得到的

$$\begin{aligned} &\sum_i m_i * u_i = 0, \\ &\sum_i m_i * v_i = 0. \end{aligned} \tag{6.4.82}$$

注释 6.4.9 在上面的方程组中, 求和号 $\sum$ 的范围是 $i \in J_n$ 或 $j \in J_n$ 上, 这可由上下文很容易地判断.

注释 6.4.10 在上面关于 u_i, v_i 等的方程组中, 为了符合实际情况, 下面的条件必须满足:

$m_0, m_1, \cdots, m_n$ 都是实数, 同时 $m_0 < 0, m_i > 0,\ i \in J_n$.

所有的 $r_{ij}((i,j) \in J_n^2)$ 都是正的实数.

对于 $i \in J_n$, u_i, v_i 是共轭复数.

$z_{ij} \neq 0, w_{ij} \neq 0$, 其中 $(i,j) \in J_n^2$.

定义 6.4.11 对于一个刚体或中心构型 $\begin{bmatrix} m_1 & m_2 & \cdots & m_n \\ \mathbf{r}_1 & \mathbf{r}_2 & \cdots & \mathbf{r}_n \end{bmatrix}$ 的实现条件是指注释 6.4.10 中的条件.

<u>决定 $n=3$ 时的刚体或中心构型</u>

当 $n=2$ 时, 刚体或中心构型的决定是简单的. 我们继续考虑 $n=3$ 时的情况, 这归结为下面例子中问题.

例 6.4.12 我们要求解方程组 (6.4.79)~(6.4.82), 其中 $n=3$. 对于变量 u_i, v_i, m_0, r_{ij}, 其中 $i \in J_3, (i,j) \in J_3^2$, 参数为 m_i, $i \in J_3$. 为了求解, 我们将变量 u_2, u_3, v_2, v_3 用 $u_{12}, u_{13}, v_{12}, v_{13}$ 以如下方式代替:

$$\left.\begin{aligned} u_{12} = u_1 - u_2,\ u_{13} = u_1 - u_3, \\ v_{12} = v_1 - v_2,\ \ v_{13} = v_1 - v_3, \end{aligned}\right\} \tag{6.4.83}$$

于是, 我们有

$$u_2 - u_3 = u_{13} - u_{12},\ \ v_2 - v_3 = v_{13} - v_{12}. \tag{6.4.84}$$

显然, 求解 (6.4.79)~(6.4.82) 等价于求解下面的 $QS=0$, 变量为 $u_1, u_{12}, u_{13}, v_1, v_{12}, v_{13}, m_0, r_{12}, r_{13}, r_{23}$, 已知参数为 m_1, m_2, m_3, 这里 $QS = \{Q_1, \cdots, Q_9\}, Q_i(i = 1, 2, \cdots, 9)$ 如下:

$$\left.\begin{aligned}
&Q_1 = u_1*(m_3+m_2+m_1) - u_{13}*m_3 - u_{12}*m_2,\\
&Q_2 = (v_{13}-v_{12})*v_{13}*r_{23}*r_{13}*(r_{12}^3*m_0+m_2+m_1)\\
&\qquad +v_{13}*v_{12}*r_{12}*m_3*(r_{23}-r_{13}) - v_{12}^2*r_{23}*r_{12}*m_3,\\
&Q_3 = v_{13}^2*r_{23}*r_{13}*m_2 + v_{13}*v_{12}*r_{23}*r_{13}*(r_{13}^2*r_{12}*m_0-m_2)\\
&\qquad +v_{13}*v_{12}*r_{12}*(r_{23}*m_3+r_{23}*m_1+r_{13}*m_2)\\
&\qquad -v_{12}^2*r_{23}*r_{12}*(r_{13}^3*m_0+m_3+m_1),\\
&Q_4 = v_1*u_{13}*u_{12}*r_{13}*r_{12}*m_0 + u_{13}*r_{13}*m_2 + u_{12}*r_{12}*m_3,\\
&Q_5 = (u_{13}-u_{12})*u_{13}*r_{23}*r_{13}*(r_{12}^3*m_0+m_2+m_1)\\
&\qquad +u_{13}*u_{12}*r_{12}*m_3*(r_{23}-r_{13}) - u_{12}^2*r_{23}*r_{12}*m_3,\\
&Q_6 = u_{13}^2*r_{23}*r_{13}*m_2 + u_{13}*u_{12}*r_{23}*r_{13}*(r_{13}^2*r_{12}*m_0-m_2)\\
&\qquad +u_{13}*u_{12}*r_{12}*(r_{23}*m_3+r_{23}*m_1+r_{13}*m_2)\\
&\qquad -u_{12}^2*r_{23}*r_{12}*(r_{13}^3*m_0+m_3+m_1),\\
&Q_7 = v_{12}*u_{12} - r_{12}^2,\qquad Q_8 = v_{13}*u_{13} - r_{13}^2,\\
&Q_9 = (v_{13}-v_{12})*(u_{13}-u_{12}) - r_{23}^2.
\end{aligned}\right\} \tag{6.4.85}$$

我们还必须遵守实现条件. 进一步说, $u_{12}, u_{13}, v_{12}, v_{13}$, $r_{12}, r_{13}, r_{23}, m_0, m_1, m_2, m_3$ 不全为 0. 令 NZ 是所有的这些非 0 变量和参数的积, 则问题就简化为判定

$$\mathrm{Zero}_{(rc)}(QS/NZ) \subset \mathrm{Zero}_{\mathbf{C}}(QS/NZ), \tag{6.4.86}$$

其中 (rc) 表示所有的零点被限制在那些实现条件必须得到满足. 为了判定 (6.4.86), 我们首先按照下面的序排列所涉及到的变量和参数:

$$m_1 \prec m_2 \prec m_3 \prec r_{12} \prec r_{13} \prec r_{23} \prec m_0 \prec u_{12} \prec u_{13} \prec v_{12} \prec v_{13} \prec u_1 \prec v_1. \tag{6.4.87}$$

现在我们利用替换法则, 将 Q_2, Q_3 用 Q_2 相对于 Q_3 的余式 Q_{10} 和 Q_2 与 Q_3 相对于 v_{13} 的结式 Q_{11} 来替换. 结式 Q_{11} 的指标集为 $[57\ m_0\ 3]$, Q_{10} 具有如下形式:

$$Q_{10} = v_{13} * g_0 + v_{12} * h_0, \tag{6.4.88}$$

其中 g_0, h_0 的指标集分别为 $[12\ m_0\ 2]$ 和 $[8\ m_0\ 2]$. 同样地, 我们将 Q_5, Q_6 分别用 Q_5 相对于 Q_6 的余式 Q_{12} 与 Q_5 和 Q_6 相对于 u_{13} 的结式 Q_{13} 来代替. 这就证明了 Q_{13} 等于 Q_{11}, 这样我们就可以去掉它, 此时 Q_{12} 具有形式

$$Q_{12} = u_{13} * g_0 + u_{12} * h_0, \tag{6.4.89}$$

相继消去 v_{13}, u_{13}, v_{12} 的过程中, 构造 Q_8 相对于 Q_{10}, Q_{12}, Q_7 的余式, 我们得到 Q_{14}, 可将其分解为

$$\left.\begin{aligned} Q_{14} &= f_a * f_b, \\ f_a &= -r_{13} * g_0 + r_{12} * h_0, \\ f_b &= +r_{13} * g_0 + r_{12} * h_0. \end{aligned}\right\} \tag{6.4.90}$$

由 $Q_{14} = 0$ 可知: $f_a = 0$ 或 $f_b = 0$. 从 Q_9 相对于 Q_8, Q_7, Q_{10}, Q_{12} 的余式, 我们得到 Q_{15} 的形式如下:

$$Q_{15} = (-r_{23}^2 + r_{13}^2 + r_{12}^2) * g_0 + 2 * r_{12}^2 * h_0. \tag{6.4.91}$$

首先考虑 $f_a = 0$ 的情况. 经过简化以后, 可以证明 Q_{15} 可以分解为三个因子 $f_{ai}(i = 1, 2, 3)$ 如下:

$$\left.\begin{aligned} f_{a1} &= g_0, \\ f_{a2} &= r_{23} - r_{13} - r_{12}, \\ f_{a3} &= r_{23} + r_{13} + r_{12}. \end{aligned}\right\} \tag{6.4.92}$$

再考虑 $f_b=0$ 的情况，则简化后，Q_{15} 就会被分解为因子 $f_{bi}(i=1,2,3)$:

$$\left.\begin{aligned} f_{b1} &= g_0, \\ f_{b2} &= r_{23}-r_{13}+r_{12}, \\ f_{b3} &= r_{23}+r_{13}-r_{12}. \end{aligned}\right\} \tag{6.4.93}$$

由上面，我们容易得到

$$\mathrm{Zero}_{(rc)}(QS/NZ)=\bigcup_{k}\mathrm{Zero}_{(rc)}(AS_k/NZ)+\bigcup_{k=1}^{3}\mathrm{Zero}_{(rc)}(BS_k/NZ). \tag{6.4.94}$$

而且

$$\left.\begin{aligned} AS_k &= QS+\{Q_{10},Q_{11},Q_{12}\}+\{f_a,f_{ak}\}, \\ BS_k &= QS+\{Q_{10},Q_{11},Q_{12}\}+\{f_b,f_{bk}\}, \end{aligned}\quad k=1,2,3.\right\} \tag{6.4.95}$$

注意到由于 $u_{12}\neq 0, v_{12}\neq 0$, 根据 (6.4.89), $(6.4.92)_1$,$(6.4.93)_1$, 集合 $\{f_a,f_{a1}\}$ 与 $\{f_b,f_{b1}\}$ 都 0- 等价于 $\{g_0,h_0\}$.

从实现条件出发，我们有 $f_{a3}\neq 0$, 所以

$$ZA_3=\mathrm{Zero}_{(rc)}(AS_3/NZ)=\emptyset. \tag{6.4.96}$$

另一方面，由我们的一般方法可得

$$\left.\begin{aligned} ZA_1 &= \mathrm{Zero}_{(rc)}(AS_1/NZ)=\mathrm{Zero}_{(rc)}(CS_{a1}/NZ), \\ ZA_2 &= \mathrm{Zero}_{(rc)}(AS_2/NZ)=\mathrm{Zero}_{(rc)}(CS_{a2}/NZ). \end{aligned}\right\} \tag{6.4.97}$$

在 (6.4.97) 中， $CS_{ak}=\{C_{ak1},\cdots,C_{ak8}\}(k=1,2)$ 都是三角列或升列，多项式 $C_{aki}(i=1,\cdots,8)$ 如下：

$$\left.\begin{aligned} C_{a11} &= r_{13}-r_{12}, \\ C_{a12} &= r_{23}-r_{12}, \\ C_{a13} &= m_0*r_{12}^3+(m_3+m_2+m_1), \\ C_{a14} &= u_{13}^2-u_{13}*u_{12}+u_{12}^2, \\ C_{a15} &= v_{12}*u_{12}-r_{12}^2, \\ C_{a16} &= v_{13}*u_{13}-r_{12}^2, \\ C_{a17} &= u_1*(m_3+m_2+m_1)-u_{13}*m_3-u_{12}*m_2, \\ C_{a18} &= v_1*u_{13}*u_{12}*r_{12}*m_0+u_{13}*m_2+u_{12}*m_3. \end{aligned}\right\} \tag{6.4.98}$$

$$\left.\begin{aligned}
C_{a21} &= r_{13}^5 * (m_2 + m_1) + r_{13}^4 * r_{12} * (3 * m_2 + 2 * m_1) \\
&\quad + r_{13}^3 * r_{12}^2 * (3 * m_2 + m_1) - r_{13}^2 * r_{12}^3 * (3 * m_3 + m_1) \\
&\quad - r_{13} * r_{12}^4 * (3 * m_3 + 2 * m_1) - r_{12}^5 * (m_3 + m_1), \\
C_{a22} &= r_{23} - r_{13} - r_{12}, \\
C_{a23} &= m_0 * r_{13}^2 * r_{12}^3 * (r_{13} + r_{12})^2 + r_{13}^2 * (r_{13} + r_{12})^2 * (m_2 + m_1) \\
&\quad - (2 * r_{13} + r_{12}) * r_{12}^3 * m_3, \\
C_{a24} &= u_{13} * r_{12} + u_{12} * r_{13},
\end{aligned}\right\} \tag{6.4.99}$$

当 $k = 5,6,7,8$ 时，C_{a2k} 等于 C_{a1k}. 从 C_{a11}, C_{a12}, 我们易知: ZA_1 给出了拉格朗日形式的中心构型，而 ZA_2 给出了欧拉形式的中心构型，其中粒子 m_1, m_2, m_3 共线，m_1 位于 m_2 与 m_3 之间. 特别地，C_{a21} 给出了一个用 $\frac{r_{13}}{r_{12}}$ 表示的五次方程在起初欧拉给出的实际条件下，它有且仅有的一个正的实数解.

集合 $ZB_1 = \mathrm{Zero}_{(rc)}(BS_1/NZ)$ 与 $ZA_1 = \mathrm{Zero}_{(rc)}(AS_1/NZ)$ 一致，而且 $ZB_k = \mathrm{Zero}_{(rc)}(BS_k/NZ)(k = 2,3)$ 与 $ZA_2 = \mathrm{Zero}_{(rc)}(AS_2/NZ)$ 类似，它们对应于其他两个共线的欧拉中心构型.

当 $n = 3$ 时，所有可能的中心构型所组成的集合，由下面所陈述的定理完全决定:

定理 6.4.13 三个质量非零的物体的仅可能的中心构型是典型的欧拉和拉格朗日型的.

涡流运动中的刚体构型

现在，我们考虑不可压缩和非粘性的且能达到无穷远处的流体中的涡流运动.

记号 6.4.14 用 $F_1, \cdots, F_n$ 代表 n 个在它们自身的影响下运动的平行直线涡流线.

用 $k_1, \cdots, k_n$ 代表 n 个涡流线 F_i 的强度.

用 P 代表一个垂直于 n 个流线 F_i 的固定平面，坐标系为 (x, y).

用 $\mathbf{r}_1, \cdots, \mathbf{r}_n$ 代表平面 P 上的涡流线 F_i 的轨迹，或从原点 O 到那条轨迹的向量.

用 $\mathbf{e}$ 代表与固定平面 P 正交的单位向量.

用 r_{ij} 代表平行流线 F_i 与 F_j 间的距离.

用 $\begin{bmatrix} k_1 & k_2 & \cdots & k_n \\ \mathbf{r}_1 & \mathbf{r}_2 & \cdots & \mathbf{r}_n \end{bmatrix}$ 代表固定平面 P 上的 n 条平行涡流线 F_i 的构型，强度为 k_i, 轨迹为 $\mathbf{r}_i$.

假设 K

$$\sum_i k_i \neq 0. \tag{6.4.100}$$

在假设 K 下，在平面 P 的有限部分存在着一个 中心, 使得如果我们将中心取为原点 O, 则我们就有

$$\sum_i k_i * \mathbf{r}_i = 0,$$

或

$$\left.\begin{aligned}\sum_i k_i * x_i = 0,\\ \sum_i k_i * y_i = 0.\end{aligned}\right\} \tag{6.4.101}$$

现在考虑涡流构型

$$\begin{bmatrix} k_1 & k_2 & \cdots & k_n \\ \mathbf{r}_1 & \mathbf{r}_2 & \cdots & \mathbf{r}_n \end{bmatrix}.$$

定义 6.4.15 $\begin{bmatrix} k_1 & k_2 & \cdots & k_n \\ \mathbf{r}_1 & \mathbf{r}_2 & \cdots & \mathbf{r}_n \end{bmatrix}$ 是一个 固定构型 当且仅当构型在其自身影响下的运动中保持不动.

定义 6.4.16 $\begin{bmatrix} k_1 & k_2 & \cdots & k_n \\ \mathbf{r}_1 & \mathbf{r}_2 & \cdots & \mathbf{r}_n \end{bmatrix}$ 是一个 刚体构型 当且仅当构型在其自身影响下的运动中仍与原始的构型保持一致.

注释 6.4.17 对于处于牛顿引力作用下的运动粒子，没有固定构型的模拟.

<u>刚体涡流构型的某些基本性质</u>

下面 $\begin{bmatrix} k_1 & k_2 & \cdots & k_n \\ \mathbf{r}_1 & \mathbf{r}_2 & \cdots & \mathbf{r}_n \end{bmatrix}$ 是一个用来证明假设 K 的涡流构型，因此系统的中心存在，我们可以取其为坐标系的原点.

命题 6.4.18 对于一个满足假设 K 的刚体涡流构型，整个构型将以一定的角速度围绕固定的中心运动.

证明 令原点 O 是固定的中心. 我们用 $\frac{c(t)}{2*\pi}$ 表示整个刚体构型绕原点 O 在某一时刻 t 的角速度，则第 i 个流线 $\mathbf{v}_i(t)$ 在时刻 t 的速度为

$$\mathbf{v}_i(t) = \frac{c(t)}{2*\pi} * (\mathbf{e} \times \mathbf{r}_i(t)).$$

现在考虑流线 F_i 的速度，由于流线 F_j 在时刻 t 的速度为

$$\mathbf{v}_{ji}(t) = \frac{1}{2*\pi} * k_j * \frac{\mathbf{e} \times (\mathbf{r}_i(t) - \mathbf{r}_j(t))}{r_{ij}^2},$$

因此，F_i 在时刻 t 的速度为

$$\mathbf{v}_i(t) = \frac{1}{2*\pi} * \sum_{j \neq i} k_j * \frac{\mathbf{e} \times (\mathbf{r}_i(t) - \mathbf{r}_j(t))}{r_{ij}^2}.$$

比较 $\mathbf{v}_i(t)$ 的两个表达式，我们有

$$\sum_{j \neq i} k_j * \frac{\mathbf{r}_i(t) - \mathbf{r}_j(t)}{r_{ij}^2} = c(t) * \mathbf{r}_i(t).$$

由于 $\mathbf{r}_i(t)$ 与 $\mathbf{r}_i(0) = \mathbf{r}_i$ 相差一个不依赖于 i 的旋转，我们得到 $c(t)$ 不依赖于 t. 因此，$\frac{c(t)}{2*\pi} = \frac{c}{2*\pi}$ 是整个刚体运动的固定的角速度. □

注释 6.4.19　由上面的证明，我们有

$$\sum_{j \neq i} k_j * \frac{\mathbf{r}_i - \mathbf{r}_j}{r_{ij}^2} = c * \mathbf{r}_i. \tag{6.4.102}$$

对应于固定涡流构型的情况，我们有 $c = 0$.

命题 6.4.20　对于固定的涡流构型必然有

$$\sum_{i \neq j} k_i * k_j = 0. \tag{6.4.103}$$

证明　由 (6.4.102) 我们可以得到

$$c * \sum_i k_i * \mathbf{r}_i^2 = \sum_{i \neq j} k_i * k_j.$$

对于固定的涡流构型 $c = 0$, 我们得 (6.4.103). □

<u>刚体涡流构型的基本方程</u>

由 (6.4.102), 我们有

$$\left.\begin{aligned} \sum_{j \neq i} k_j * \frac{x_{ij}}{r_{ij}^2} &= c * x_i, \\ \sum_{j \neq i} k_j * \frac{y_{ij}}{r_{ij}^2} &= c * y_i, \end{aligned} \quad i \in J_n. \right\} \tag{6.4.104}$$

我们引入 u_i, v_i, z_{ij}, w_{ij} 如下:

$$\left.\begin{aligned} &u_i = x_i + \mathbf{i} * y_i,\ v_i = x_i - \mathbf{i} * y_i,\ i \in J_n,\\ &z_{ij} = \frac{1}{u_i - u_j},\ w_{ij} = \frac{1}{v_i - v_j},\ (i,j) \in J_n^2,\\ &k_0 \ = \ -c, \end{aligned}\right\} \tag{6.4.105}$$

则 (6.4.104) 就变成了下面的方程:

$$\left.\begin{aligned} &k_0 * u_i + \sum_{j\neq i} k_j * w_{ij} = 0,\\ &k_0 * v_i + \sum_{j\neq i} k_j * z_{ij} = 0, \end{aligned}\quad i \in J_n.\right\} \tag{6.4.106}$$

$$\left.\begin{aligned} &(u_i - u_j) * z_{ij} - 1 = 0,\\ &(v_i - v_j) * w_{ij} - 1 = 0,\\ &r_{ij}^2 - (u_i - u_j) * (v_i - v_j) = 0, \end{aligned}\quad (i,j) \in J_n^2.\right\} \tag{6.4.107}$$

$$r_{ij} - r_{ji} = 0,\ z_{ij} + z_{ji} = 0,\ w_{ij} + w_{ji} = 0,\ \ (i,j) \in J_n^2. \tag{6.4.108}$$

我们还可以加入下面的方程:

$$\begin{aligned} &\sum_i k_i * u_i = 0,\\ &\sum_i k_i * v_i = 0. \end{aligned} \tag{6.4.109}$$

(6.4.106) 至 (6.4.109) 中所涉及的所有的变量和参数都受某些 实现条件 的限制, 即

$k_1, \cdots, k_n$ 非零实数, 而且 k_0 也为实数.

u_i, v_i 互为复共轭, $i \in J_n$.

r_{ij} 是正的实数, $(i,j) \in J_n^2$.

z_{ij}, w_{ij} 不都为零, $(i,j) \in J_n^2$.

r 实际上等于 1.

<u>确定 $n=3$ 时的刚体涡流构型</u>

将 (6.4.105)~(6.4.109) 与 (6.4.77)~(6.4.82) 比较, 我们看到确定刚体涡流构型与刚体行星构型的相同. 特别地, 我们考虑 $n=3$ 时.

例 6.4.21 我们解 $n = 3$ 时的方程组 (6.4.106)~(6.4.109), 它的变量为 $u_i, v_i, k_0, r_{ij}, i \in J_3, (i,j) \in J_3^2$, 参数为 $k_i (i \in J_3)$ 表示.

对于固定的构型, 我们有 $k_0 = -c = 0$, 而且求解十分简单. 因此下面我们仅考虑 $k_0 \neq 0$ 时的情况.

为此, 我们像以前一样, 根据 (6.4.83), (6.4.84) 中把 u_2, u_3, v_2, v_3 用 $u_{12}, u_{13}, v_{12}, v_{13}$ 代替, 则求解 (6.4.106)~(6.4.109) 相当于求解实现条件下的 $QS = 0$, 其中 $QS = \{Q_1, \cdots, Q_9\}$, $Q_i (i = 1, 2, 3, \cdots, 9)$ 如下:

$$\left.\begin{aligned}
Q_1 &= u_1 * (k_3 + k_2 + k_1) - u_{13} * k_3 - u_{12} * k_2,\\
Q_2 &= (v_{13} - v_{12}) * v_{13} * (k_0 * r_{12}^2 + k_2 + k_1) - v_{12}^2 * k_3,\\
Q_3 &= v_{13}^2 * k_2 + (v_{13} - v_{12}) * v_{12} * (k_0 * r_{13}^2 + k_3 + k_1),\\
Q_4 &= v_1 * u_{13} * u_{12} * k_0 + u_{13} * k_2 + u_{12} * k_3,\\
Q_5 &= (u_{13} - u_{12}) * u_{13} * (k_0 * r_{12}^2 + k_2 + k_1) - u_{12}^2 * k_3,\\
Q_6 &= u_{13}^2 * k_2 + (u_{13} - u_{12}) * u_{12} * (k_0 * r_{13}^2 + k_3 + k_1),\\
Q_7 &= v_{12} * u_{12} - r_{12}^2,\\
Q_8 &= v_{13} * u_{13} - r_{13}^2,\\
Q_9 &= (v_{13} - v_{12}) * (u_{13} - u_{12}) - r_{23}^2.
\end{aligned}\right\} \qquad (6.4.110)$$

我们要判定是否

$$\mathrm{Zero}_{(rc)}(QS/NZ) \subset \mathrm{Zero}_{\mathbb{C}}(QS/NZ), \qquad (6.4.111)$$

其中 (rc) 意味着零点必须满足相关的实现条件, NZ 是非零变量与参数 k_0, k_1, k_2, k_3, r_{12}, r_{13}, r_{23} 的积.

像例 6.4.12 中那样将变量排序, 用 m_i 代替 k_i, 最后我们得到下面的结果:

$$\mathrm{Zero}_{(rc)}(QS/NZ) = \bigcup_{k=1,2,3,4} \mathrm{Zero}_{(rc)}(CS_k/NZ), \qquad (6.4.112)$$

在 (6.4.112) 中, 对于每一个 k, 我们有 $CS_k = \{C_{k1}, \cdots, C_{k8}\}$, 其中 C_{ki} 如下:

$$\left.\begin{aligned}
C_{11} &= r_{13} - r_{12},\\
C_{12} &= r_{23} - r_{12},\\
C_{13} &= k_0 * r_{12}^2 + (k_3 + k_2 + k_1),\\
C_{14} &= u_{13}^2 - u_{13} * u_{12} + u_{12}^2,\\
C_{15} &= v_{12} * u_{12} - r_{12}^2,\\
C_{16} &= v_{13} * u_{13} - r_{12}^2,\\
C_{17} &= u_1 * (k_3 + k_2 + k_1) - u_{13} * k_3 - u_{12} * k_2,\\
C_{18} &= v_1 * u_{13} * u_{12} * k_0 + u_{13} * k_2 + u_{12} * k_3.
\end{aligned}\right\} \qquad (6.4.113)$$

$$\left.\begin{aligned}C_{21}&=r_{13}^3*(k_2+k_1)+r_{13}^2*r_{12}*(2*k_2+k_1)\\&\quad-r_{13}*r_{12}^2*(2*k_3+k_1)-r_{12}^3*(k_3+k_1),\\C_{22}&=r_{23}-r_{13}-r_{12},\\C_{23}&=k_0*r_{13}*r_{12}^2*(r_{13}+r_{12})+r_{13}^2*(k_2+k_1)\\&\quad+r_{13}*r_{12}*(k_2+k_1)-r_{12}^2*k_3,\\C_{24}&=u_{13}*r_{12}+u_{12}*r_{13},\end{aligned}\right\}\tag{6.4.114}$$

同时，当 $i=5,6,7,8$ 时，C_{2i} 与 C_{1i} 相同.

多项式集 CS_3, CS_4 与 CS_2 一样. CS_1 的零点集与拉格朗日的情况相似，而 CS_2, CS_3, CS_4 的零点集与行星运动中的欧拉情况相似.

我们将结果总结为下面的定理：

定理 6.4.22 对于处于不可压缩且非粘性的、能延伸到无穷远处的流体中的三个平行涡流线，如果流体的强度非零并能够满足假设 K，它们的可能的刚体构型只能为拉格朗日等变型或者欧拉直线型.

注释 6.4.23 尽管 k_1, k_2, k_3 不等于 0，但是由于它们可能为正的或负的，因此，当在相应的直线型的涡流运动中 $C_{21}=0$ 可能 1 个，或 2 个，或 3 个正的实根，或无这样的根. 而直线型的行星运动的构型唯一.

§6.5 机器人学中逆运动方程的求解

机器人描述

我们把机器人学中常用的一些术语列在下面.

定义 6.5.1 一个 n- 机器人或 n- 操纵器是通过关节将 n- 个臂连结起来的开连杆.

机器人的棱形或转动关节是两个相继臂的连结法，臂可以沿着或围绕这个轴运动. 机器人的手或终端效应器是指开连杆的终端. $6R$- 机器人是有 6 个转动轴的机器人. 其他类似，例如，$RRRRPR$- 机器人是这样的机器人，其先有 4 个转动关节，然后有一个棱形关节，最后是一个转动关节. 为明确起见，这里只考虑 $6R$- 机器人，所以，以下所说 6- 机器人均指 $6R$- 机器人. 通过适当的修改，涉及棱形轴的情形也可以处理.

记号 6.5.2 参看图 6.1.

假设第 $i-1, i, i+1$ 三个相继的关节的轴互不相交，则用 J_{i-1}, J_i, J_{i+1} 分别记这三个关节轴.

H_iO_i，代表 J_i 与 J_{i+1} 的公垂线，其中 H_i 在 J_i 上，O_i 在 J_{i+1} 上. 定向是

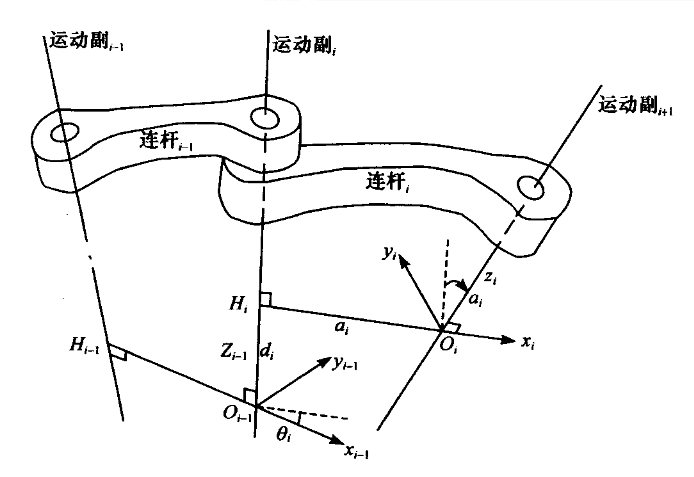


图 6.1 机器人学中逆运动方程的求解

从 H_i 到 O_i. $H_{i-1}O_{i-1}$ 的含义类同.

a_i, 代表 H_iO_i 的从 H_i 到 O_i 测量的有向长.

d_i, 代表沿有向轴 J_i 从 O_{i-1} 到 H_i 的有向距离.

α_i, 代表从有向轴 J_i 在 H_i 点的有向平行线和有向轴 J_{i+1} 在点 O_i 的有向平行线构成的有向角.

θ_i, 代表在 O_{i-1} 点的有向直线 (从 H_{i-1} 到 O_{i-1} 的方向上) 和在点 O_{i-1} 的平行线 (沿着从 H_i 到 O_i 的方向) 构成的有向角.

注释 6.5.3 角 α_i, θ_i 只可能相差 $2*\pi$ 的倍数.

注释 6.5.4 当 J_i 与 J_{i+1} 互相平行时, 将有无数多条可能的公垂线, 它们中的任何一条都可以取作 H_iO_i, 其中 H_i 在 J_i 上, O_i 在 J_{i+1} 上.

注释 6.5.5 当 J_i 与 J_{i+1} 相交于一点时, 这个点将被取作 $H_i = O_i$, 而且公垂线 H_iO_i 将被理解为通过点 H_iO_i 垂直于由 J_i 和 J_{i+1} 确定的平面, 而且是以某种方式定向的.

定义 6.5.6 d_i, a_i, α_i 称为机器人的几何约束, 它们是内在的参数. θ_i 称为机器人的控制参数.

<u>与机器人相关的几何空间和映射</u>

考虑一个机器人:

定义 6.5.7 构形空间 $\mathbf{H}$ 是指机器人手的所有可能位置的空间.

定义 6.5.8 控制空间 Θ 是指控制参数 $\theta_1, \cdots, \theta_n$ 的空间.

定义 6.5.9 机器人映射是指对应

$$\phi_n : \Theta_n \rightarrow \mathbf{H}, \tag{6.5.115}$$

$\phi_n(\theta_1,\cdots,\theta_n)$ 代表机器人手的位置是由控制参数 $\theta_1,\cdots,\theta_n$ 唯一确定的.

定义 6.5.10 机器人的值域是指映射 ϕ_n 的像.

注释 6.5.11 Θ_n 是一个实 n 维的环面; $\mathbf{H}$ 是实 3 维空间中刚体运动群空间, 维数为 6.

注释 6.5.12 ϕ_n 是多对一映射, 其像集通常情况下是 $\mathbf{H}$ 的子集, 具有维数 n.

注释 6.5.13 对于 $n=6$, 一个像点的逆像一般情况下是 Θ_n 的一个有限子集. 梁崇高首先证明, 对于一般 6- 机器人, 逆像中的点数, 如果不是无穷大, 一般是 16.

设 $n=6$, 我们将把 ϕ_n 简写为 ϕ, 其他类似. 当 Θ 中的点沿一路径变化时, 其像点在 $\mathbf{H}$ 中一般也将沿一路径变化. 但是也有例外. 为此我们给出下述定义.

定义 6.5.14 6- 机器人的一个 *手位置* 是机器人值域中的一个点 $P=\phi(\theta)$, 对于某个 $\theta\in\Theta$.

定义 6.5.15 6- 机器人的一个 *一般手位置* 是指手位置 P_0, 使得在 Θ 中只有有限个不同的点 $\theta_0^{(j)}$, 具有性质 $\phi(\theta_0^{(j)})=P_0$, 而且满足下述条件: 对于每个点 $\theta_0^{(j)}$, 存在邻域 $N_0^{(j)}$, 使得机器人映射 ϕ 是从 $N_0^{(j)}$ 到 P_0 的某个邻域 N 的局部同胚, 而且所有的邻域 $N_0^{(j)}$ 都是互不相交.

注释 6.5.16 由定义推出, 当机器人的手沿着机器人手位置的一条路径 $P_t(t\in(-t_0,+t_0),\ t_0>0)$ 充分通过一般手位置 P_0 时, $\phi^{-1}(P_0)$ 的每一个 $\theta_0^{(j)}$ 将经历一条路径 $\theta_t^{(j)}$, 而且, 所有这些路径是彼此不相交的.

定义 6.5.17 6- 机器人的一个 *奇异手位置* 是指机器人的手位置不是一般手位置.

在 6- 机器人的所有奇异手位置中, 我们引用下面一些手位置.

定义 6.5.18 6- 机器人的一个 *分歧手位置* 是指机器人的手位置 P_0, 使得存在路径 P_t 与 $\theta_t',\theta_t'',t\in(-t_0,0],t_0>0$, 对于 $t\in(-t_0,0]$, 满足 $\phi(\theta_t')=\phi(\theta_t'')=P_t$, 而且对于 $t\in(-t_0,0)$, $\theta_t'\neq\theta_t''$ 而 $\theta_0'=\theta_0''$.

定义 6.5.19 6- 机器人的一个 *死位置* 是指机器人的手位置 P_0, 使得存在一些路径 P_t 和 $\theta_t,t\in(-t_0,0],t_0>0$, 满足 $\phi(\theta_t)=P_t$, 它们不能被扩展成光滑的路径 θ_t 和 $P_t,t\in(-t_0,+t_1),t_1>0$, 满足 $\phi(\theta_t)=P_t$.

定义 6.5.20 6- 机器人的一个 *退化位置* 是机器人的手位置 P_0, 满足 $\phi^{-1}(P_0)$ 是无限集.

对于一个 6- 机器人，知道它的值域和所有可能的奇异手位置是很重要的.

机器人学的一些一般性问题

问题 R1 在构形空间 **H** 中确定值域.

问题 R2 给定构形空间 **H** 中的一个点，在 Θ 中求它的所有逆像.

问题 R3 确定所有奇异位置的集合. 特别地，分别确定所有分歧位置的集合、所有死位置的集合、和所有退化位置的集合.

Denavit-Hartenberg 坐标系

记号 6.5.21 (参看图 6.1) 用 $F_0 = OX_0Y_0Z_0$ 代表一个附在机器人上的固定坐标系 (架), 其中 $J_0 = J_1$ 为有向 OZ_0 轴.

用 $F_i = OX_iY_iZ_i (0 < i \le 6)$ 代表第 i 个坐标系 (架), 其中 O_iX_i 沿着由 H_i 到 O_i 的方向, O_iZ_i 沿着有向轴 J_{i+1} 的方向，而 F_i 的定向类似于 F_0 的定向；标架 F_6 附在机器人手上.

用 $A_{i,j}$ 代表第 j 个标架 F_j 关于第 i 个标架 F_i 的矩阵.

定义 6.5.22 n- 机器人的 Denavit-Hartenberg *坐标系 (架)* 是指坐标系 (标架)$OX_iY_iZ_i = F_i (i = 1, \cdots, n)$.

根据机器人学中的用法，我们用一个 4×4 矩阵来记一个特定的变换，其最后一行是 $(0,0,0,1)$, 左上角的 3×3 矩阵是旋转部分，最后一列，除去最下面的元素 1 后，是平移向量. 我们有

定理 6.5.23

$$A_{i-1,i} = \begin{bmatrix} \cos\theta_i & -\sin\theta_i * \cos\alpha_i & \sin\theta_i * \sin\alpha_i & a_i * \cos\alpha_i \\ \sin\theta_i & \cos\theta_i * \cos\alpha_i & -\cos\theta_i * \sin\alpha_i & a_i * \sin\alpha_i \\ 0 & \sin\alpha_i & \cos\alpha_i & d_i \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad (6.5.116)$$

$$A_{i,i-1} = \begin{bmatrix} \cos\theta_i & \sin\theta_i & 0 & -a_i \\ -\sin\theta_i * \cos\alpha_i & \cos\theta_i * \cos\alpha_i & \sin\alpha_i & -d_i * \sin\alpha_i \\ \sin\theta_i * \sin\alpha_i & -\cos\theta_i * \sin\alpha_i & \cos\alpha_i & -d_i * \cos\alpha_i \\ 0 & 0 & 0 & 1 \end{bmatrix}. \quad (6.5.117)$$

证明 这结论可从如下等式推出：

$$A_{i-1,i} = \mathrm{Rot}(OZ_i, \theta_i) \circ \mathrm{Trans}(0,0,d_i) \circ \mathrm{Trans}(a_i,0,0) \circ \mathrm{Rot}(OX_i, \alpha_i), \quad (6.5.118)$$

其中 $\mathrm{Rot}(J,\lambda)$ 是绕有向轴 J 旋转一个有向角 λ 的旋转，$\mathrm{Trans}(v)$ 表示沿向量 v 的平移. □

<u>逆运动方程</u>

依照上述问题，我们可以提出一个更为简单的问题：

问题 R4 假设机器人的手位置已知，求控制参数 θ_i，使得机器人的手恰在已知的位置.

假设已知手位置由矩阵

$$H = A_{0,6} = \begin{bmatrix} h_{11} & h_{21} & h_{31} & h_{41} \\ h_{12} & h_{22} & h_{32} & h_{42} \\ h_{13} & h_{23} & h_{33} & h_{43} \\ 0 & 0 & 0 & 1 \end{bmatrix} \tag{6.5.119}$$

给出，则问题等价于解关于 θ_i 的下列方程：

$$A_{01} \circ A_{12} \circ \cdots \circ A_{56} = H, \tag{6.5.120}$$

其中 h_{ij} 已知.

定义 6.5.24 n- 机器人的逆运动方程是指关于 θ_i 的方程 (6.5.120)，假定 H 已知.

利用这一定义，问题 R4 可以陈述为

问题 R4′ 利用 h_{ij}，解关于 θ_i 的方程 (6.5.120).

注释 6.5.25 由 (6.5.119) 可知，机器人的构形空间可以看作是以 $h_{ij}(i=1,2,3,4;\ j=1,2,3)$ 为坐标的 12 维实空间 $\mathbf{R}^{12}$ 中满足 (3×3) 矩阵 $(h_{ij})_{i,j=1,2,3}$ 是正交矩阵的条件的 6 维子空间.

<u>Puma 型机器人</u>

一般的 6- 机器人逆运动方程的求解是非常复杂的，所以我们将仅讨论几种简单类型的机器人.

定义 6.5.26 一个 $6R$- 机器人称为是 Puma 型的当且仅当 6 个关节轴的相继对或是相互平行，或是相互垂直.

总共有 2^5 个不同的 Puma 型机器人. 为明确起见，我们考虑 Puma 机器人

$$J_1 \perp J_2 \parallel J_3 \perp J_4 \perp J_5 \perp J_6. \tag{6.5.121}$$

定义 6.5.27 Puma 型机器人是指满足条件 (6.5.121) 的 $6R$- 机器人. 参看图 6.2.

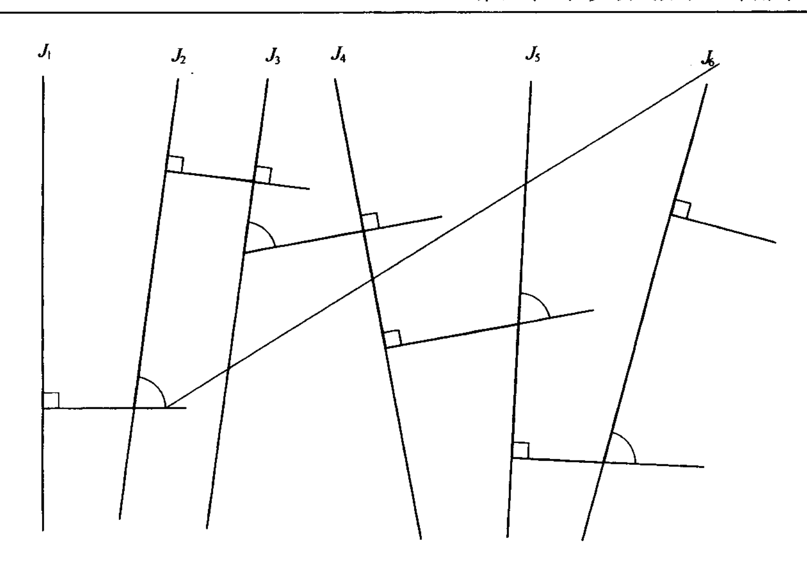


图 6.2 Puma 型机器人

<u>Puma 型机器人的逆运动方程</u>

对于 Puma 型机器人，我们首先给关节轴和 O_iH_i 以这样的方式定向，使得所有的直角 α_i 均为 $+\frac{\pi}{2}$. 这样相继的约束角将是

$$(\alpha_1, \alpha_2, \cdots, \alpha_6) = \left(+\frac{\pi}{2}, 0, +\frac{\pi}{2}, +\frac{\pi}{2}, +\frac{\pi}{2}, 0\right). \tag{6.5.122}$$

此外，我们还将选择标架 F_0 和 F_6, 使得 O_0Z_0 位于有向轴 J_1 上，而且与之同向, $O_6 = H_6$ 与 O_5 重合, O_6Z_6 与 O_5Z_5 具有相同的方向. 由此引出简化方程:

$$d_6 = 0. \tag{6.5.123}$$

现在令

$$\left.\begin{aligned} &c_i = \cos\theta_i, \quad s_i = \sin\theta_i, \quad i = 1, 3, 4, 5, 6, \\ &c_{23} = \cos\theta_{23}, \quad s_{23} = \sin\theta_{23}, \\ &\theta_{23} = \theta_2 + \theta_3, \quad d_{23} = d_2 + d_3, \end{aligned}\right\} \tag{6.5.124}$$

则求解 Puma R- 机器人的问题等价于利用 a_i, d_i 求解 $c_i, s_i (i \neq 2)$ 和 c_{23}, s_{23}, 而 H_{ij} 看作是已知参数. 为此，我们用一个与 (6.5.120) 等价的方程

$$A_{34} \circ A_{45} \circ A_{56} = A_{32} \circ A_{21} \circ A_{10} \circ H \tag{6.5.125}$$

代替方程 (6.5.120).

为简单起见，我们引进多项式:

$$\left.\begin{aligned}&f_{i1}=s_1*h_{i2}+c_1*h_{i1}-\delta_{4i}*a_1, \quad && i=1,2,3,4,\\&f_{i2}=-s_1*h_{i1}+c_1*h_{i2}+\delta_{4i}*d_{23}, && i=1,2,3,4,\\&f_{43}=h_{43}-d_1,\end{aligned}\right\}\tag{6.5.126}$$

由此得到多项式组：$P_i=0, i=1,\cdots,12$, 其中

$$\left.\begin{aligned}&P_1=s_6*s_4+c_6*c_5*-s_{23}*h_{13}-c_{23}*f_{11},\\&P_2=s_6*c_4-c_6*c_5*s_4-f_{12},\\&P_3=c_6*s_5-s_{23}*f_{11}+c_{23}*h_{13},\\&P_4=s_6*c_5*c_4-c_6*s_4+s_{23}*h_{23}+c_{23}*f_{21},\\&P_5=s_6*c_5*s_4+c_6*c_4-f_{22},\\&P_6=s_6*s_5+s_{23}*f_{21}-c_{23}*h_{23},\\&P_7=s_5*c_4-s_{23}*h_{33}-c_{23}*f_{31},\\&P_8=s_5*s_4+f_{32},\\&P_9=c_5+s_{23}*f_{31}-c_{23}*h_{33},\\&P_{10}=c_5*c_4*a_5+s_4*d_5+c_4*a_4+c_3*a_2-s_{23}*f_{43}\\&\qquad -c_{23}*f_{41}+a_3,\\&P_{11}=c_5*s_4*a_5+s_4*a_4-c_4*d_5+f_{42},\\&P_{12}=s_5*a_5+s_3*a_2-s_{23}*f_{41}+c_{23}*f_{43}+d_4.\end{aligned}\right\}\tag{6.5.127}$$

除此之外，对于三角函数我们还有三角恒等式：$P_i=0, i=13,\cdots,18$, 其中

$$\left.\begin{aligned}&P_i=c_{i-12}^2+s_{i-12}^2-1, \quad i=13,15,16,17,18,\\&P_{14}=c_{23}^2+s_{23}^2-1.\end{aligned}\right\}\tag{6.5.128}$$

于是, Puma 机器人的问题 R4 等价于确定多项式集

$$PS=\{P_1,\cdots,P_{18}\}\tag{6.5.129}$$

的零点集 Zero(PS).

Puma 机器人多项式零点集 Zero(PS) 的初步简化

为了解方程组 $PS=0$, 即确定零点集 Zero(PS), 考虑到简化计算，我们先做些初步的变换. 借助于方程 $P_{16}=0$, 多项式 P_1 和 P_2 分别 0 - 等价于多项式 P_1' 和 P_2', 其中

$$P_1' = s_4 * P_1 + c_4 * P_2, \quad P_2' = s_4 * P_1 - c_4 * P_2. \tag{6.5.130}$$

类似地, 多项式对 P_4, P_5 和 P_7, P_8 分别 0- 等价于多项式对 P_4', P_5' 和 P_7', P_8', 其中

$$\left.\begin{aligned} P_4' &= -s_4 * P_4 + c_4 * P_5, \quad P_5' = c_4 * P_4 + s_4 * P_5, \\ P_7' &= s_4 * P_7 - c_4 * P_8, \quad\;\; P_8' = c_4 * P_7 + s_4 * P_8. \end{aligned}\right\} \tag{6.5.131}$$

进一步地, 多项式对 P_2', P_3 和 P_5', P_6 分别 0- 等价于多项式对 P_2'', P_3' 与 P_5'', P_6', 其中

$$\left.\begin{aligned} P_2'' &= s_5 * P_2' - c_5 * P_3, \quad P_3' = c_5 * P_2' + s_5 * P_3, \\ P_5'' &= s_5 * P_5' - c_5 * P_6, \quad P_6' = c_5 * P_5' + s_5 * P_6. \end{aligned}\right\} \tag{6.5.132}$$

将 P_i 写成 P_i', $i \geq 9$, 重写 P_2'', P_5'' 成 P_2', P_5', 则多项式集 PS 0- 等价于多项式集

$$PS' = \{P_1', \cdots, P_{18}'\}, \tag{6.5.133}$$

其中

$$\left.\begin{aligned}
P_1' &= s_6 - c_4 * f_{12} - s_4 * c_{23} * f_{11} - s_4 * s_{23} * h_{13}, \\
P_2' &= c_6 - c_5 * c_4 * (c_{23} * f_{11} - s_{23} * h_{13}) \\
&\quad c_5 * s_4 * f_{12} + s_5 * c_{23} * h_{13} - s_5 * s_{23} * f_{11}, \\
P_3' &= -c_5 * c_{23} * h_{13} + c_5 * s_{23} * f_{11} - s_5 * c_4 * c_{23} * f_{11} \\
&\quad -s_5 * c_4 * s_{23} * h_{13} + s_5 * s_4 * f_{12}, \\
P_4' &= c_6 - c_4 * f_{22} - s_4 * c_{23} * f_{21} - s_4 * s_{23} * h_{23}, \\
P_5' &= s_6 + c_5 * c_4 * c_{23} * f_{21} + c_5 * c_4 - s_5 * s_{23} * h_{23} \\
&\quad -c_5 * s_4 * f_{22} - s_5 * c_{23} * h_{23} + s_5 * s_{23} * f_{21}, \\
P_6' &= c_5 * c_{23} * h_{23} - c_5 * s_{23} * f_{21} + s_5 * c_4 * c_{23} * f_{21} \\
&\quad +s_5 * c_4 * s_{23} * h_{23} - s_5 * s_4 * f_{22}, \\
P_7' &= c_4 * f_{32} + s_4 * c_{23} * f_{31} + s_4 * s_{23} * h_{33}, \\
P_8' &= s_5 - c_4 * c_{23} * f_{31} - c_4 * s_{23} * h_{33} + s_4 * f_{32}, \\
P_i' &= P_i, \quad i = 9, \cdots, 18.
\end{aligned}\right\} \tag{6.5.134}$$

这样, 求 Zero(PS) 等价于求 Zero(PS').

一个特殊的 Puma R- 机器人 —— Puma 560

目前使用的更为特殊的 Puma 型机器人是 Puma560. 定义如下:

定义 6.5.28　Puma560 是一个 $6R$- 机器人, 其关节轴 J_i 还满足下列关系:

$$J_4, J_5, J_6\text{平行而且任何两个都不重合.} \tag{6.5.135}$$

条件 (6.5.135) 以及机器人手所处的自然几何形态蕴涵

$$a_4 = a_5 = d_5 = 0. \tag{6.5.136}$$

另一方面，我们将假定

$$a_2, a_3, d_{23}, d_4 \text{ 均不为零.} \tag{6.5.137}$$

于是，(6.5.133) 中的多项式 $P'_{10}, P'_{11}, P'_{12}$ 将被简化为下列形式：

$$\left.\begin{aligned} P'_{10} &= c_3 * a_2 - s_{23} * f_{43} - c_{23} * f_{41} + a_3, \\ P'_{11} &= s_1 * h_{41} - c_1 * h_{42} - d_{23}, \\ P'_{12} &= s_3 * a_2 - s_{23} * f_{41} + c_{23} * f_{43} + d_4. \end{aligned}\right\} \tag{6.5.138}$$

Puma560 的多项式集 PS 或 PS' 的特征集

现在，我们引进诸变量 c, s 的序如下：

$$s_1 < c_1 < s_{23} < c_{23} < s_4 < c_4 < s_5 < c_5 < s_6 < c_6 < s_3 < c_3, \tag{6.5.139}$$

则特征集算法很容易给出其三角化集 (也很容易转化成特征集，如果需要的话)

$$CS = \{C_1, \cdots, C_{12}\}, \tag{6.5.140}$$

其中 C_i 给出如下：

$$\left.\begin{aligned}
C_1 &= s_1^2 * (h_{42}^2 + h_{41}^2) - 2 * s_1 * h_{41} d_{23} - h_{42}^2 + d_{23}^2, \\
C_2 &= c_1 * h_{42} - s_1 * h_{41} + d_{23}, \\
C_3 &= 4 * s_{23}^2 * (f_{43}^2 + f_{41}^2) * (d_4^2 + a_3^2) \\
&\quad -4 * s_{23} * (f_{43} * a_3 + f_{41} * d_4) * (f_{23}^2 + f_{41}^2 + d_4^2 + a_3^2 - a_2^2) \\
&\quad +(f_{23}^2 + f_{41}^2 + d_4^2 + a_3^2 - a_2^2)^2 - 4 * (f_{43} * d_4 - f_{41} * a_3)^2, \\
C_4 &= 2 * c_{23} * (f_{43} * d_4 - f_{41} * a_3) - 2 * s_{23} * (f_{43} * a_3 + f_{41} * d_4) \\
&\quad +f_{43}^2 + f_{41}^2 + d_4^2 + a_3^2 - a_2^2, \\
C_5 &= s_4^2 * (c_{23} * f_{31} + s_{23} * h_{33})^2 + s_4^2 * f_{23}^2 - f_{32}^2, \\
C_6 &= c_4 * f_{32} + s_4 * c_{23} * f_{31} + s_4 * s_{23} * h_{33}, \\
C_7 &= s_5 - c_4 * c_{23} * f_{31} - c_4 * s_{23} * h_{33} + s_4 * f_{32}, \\
C_8 &= c_5 - c_{23} * h_{33} + s_{23} * f_{31}, \\
C_9 &= s_6 - c_4 * f_{12} - s_4 * c_{23} * f_{11} - s_4 * s_{23} * h_{13}, \\
C_{10} &= c_6 - c_4 * f_{22} - s_4 * c_{23} * f_{21} - s_4 * s_{23} * h_{23}, \\
C_{11} &= s_3 * a_2 + c_{23} * f_{43} - s_{23} * f_{41} + d_4, \\
C_{12} &= c_3 * a_2 - c_{23} * f_{41} - s_{23} * f_{43} + a_3.
\end{aligned}\right\} \tag{6.5.141}$$

去掉一些非零因子后，诸 C_i 的非平凡初式为:

$$\begin{aligned}
I_1 &= h_{42}^2 + h_{41}^2,\\
I_2 &= h_{42},\\
I_3 &= f_{43}^2 + f_{41}^2,\\
I_4 &= f_{43} * d_4 - f_{41} * a_3,\\
I_5 &= (c_{23} * f_{31} + s_{23} * h_{33})^2 + f_{32}^2,\\
I_6 &= f_{32}.
\end{aligned} \tag{6.5.142}$$

注意到，因为 $C_2 = 0$ 和 $d_{23} \neq 0$, 所以实解 $I_1 \neq 0$. 进一步地， $I_6 \neq 0$ 意味着 $I_5 \neq 0$, $I_3 = 0$ 意味着 $f_{43} = f_{41} = 0$, 所以 $I_4 = 0$. 于是由整序原理得到:

定理 6.5.29 对于 Puma560, 与逆运动方程 $PS = 0$ 相应的 (6.5.127) 中多项式集 PS 的特征集 CS 可由 (6.5.140) 和 (6.5.141) 给出，而且

$$\begin{aligned}
\mathrm{Zero}_{\mathbf{R}}(PS) = {} & \mathrm{Zero}_{\mathbf{R}}(CS/f_{32} * h_{42} * I_4)\\
& + \mathrm{Zero}_{\mathbf{R}}(PS + \{h_{42}\}) + \mathrm{Zero}_{\mathbf{R}}(PS + \{f_{32}\})\\
& + \mathrm{Zero}_{\mathbf{R}}(PS + \{I_4\}).
\end{aligned} \tag{6.5.143}$$

(6.5.143) 中后三个零点集的求解可以由我们的一般算法得出，这里将不予考虑. 从特征集的形式可以看出，对于给定的手位置，几何上至多有 8 个可能的实解，而且，Puma560 的奇异性可通过初式的零点或 CS 的判别式来研究.

<u>Puma560 初式为零的退化情形</u>

确定 (6.5.143) 右端最后三个零点集是件非常烦琐的事情. 换一种做法，我们将直接由 CS 的表达式给出一些结论. 为此目的，我们列出一些初等引理. 这里我们只感兴趣实解.

引理 6.5.30 设 $A, B, C \in \mathbf{R}, A, B$ 不全为零，而且

$$A * \cos\theta + B * \sin\theta + C = 0, \tag{6.5.144}$$

则 (6.5.144) 关于 θ 有解的充要条件是

$$A^2 + B^2 - C^2 \geq 0. \tag{6.5.145}$$

在有解的情形，我们有

$$\left.\begin{aligned}
\sin\theta &= \frac{-B * C + \varepsilon * A * \sqrt{A^2 + B^2 - C^2}}{A^2 + B^2},\\
\cos\theta &= \frac{-A * C - \varepsilon * B * \sqrt{A^2 + B^2 - C^2}}{A^2 + B^2},
\end{aligned}\right\} \tag{6.5.146}$$

其中 $\varepsilon = \pm 1$.

证明是初等的，此略.

由 (6.5.145), 有必要列出如下定义.

定义 6.5.31 (6.5.144) 左端的判别式定义为 $A^2 + B^2 - C^2$.

引理 6.5.32 如果 $f_{32} = 0$, 则

$$N_1 \equiv (h_{32} * h_{41} - h_{31} * h_{42})^2 - (h_{31}^2 + h_{32}^2) * d_{23}^2 = 0. \tag{6.5.147}$$

证明 由 (6.5.126) 有

$$f_{32} = -s_1 * h_{31} + c_1 * h_{32} = 0.$$

因为 $\mathrm{Zero}(PS) = \mathrm{Zero}(PS') \subset \mathrm{Zero}(CS)$, 由 (6.5.141), 我们还有

$$C_2 = c_1 * h_{42} - s_1 * h_{41} + d_{23} = 0,$$

因而

$$c_1 * (h_{42} * h_{31} - h_{41} * h_{32}) = -h_{31} * d_{23},$$
$$s_1 * (h_{42} * h_{31} - h_{41} * h_{32}) = -h_{32} * d_{23},$$

由此容易得到 (6.5.147). □

引理 6.5.33 如果 $I_4 = f_{43} * d_4 - f_{41} * a_3 = 0$, 则 $h_{41} = h_{42} = 0$, 或者

$$N_2 \equiv (h_{42}^2 + h_{41}^2) - (f_{43} * d_4 + a_1 * a_3)^2 - d_{23}^2 = 0. \tag{6.5.148}$$

证明 由 (6.5.126) 及 $I_4 = 0$ 有

$$c_1 * h_{41} + s_1 * h_{42} + d_{23} - (f_{43} * d_4 + a_1 * a_3) = 0.$$

结合 $C_2 = 0$ 得

$$c_1 * (h_{42}^2 + h_{41}^2) = (f_{43} * d_4 + a_1 * a_3) * h_{41} - h_{42} * d_{23},$$
$$s_1 * (h_{42}^2 + h_{41}^2) = (f_{43} * d_4 + a_1 * a_3) * h_{42} - h_{41} * d_{23}.$$

因而我们得到

$$(h_{42}^2 + h_{41}^2) * N_2 = 0.$$

引理容易得证. □

注释 6.5.34 如果 $N_2 = 0$, 则 h_{41}, h_{42} 不能同时为零，这是因为 d_{23} 假定不为零.

定理 6.5.35 如果 h_{42}, N_1, N_2 都不为零，则

$$\mathrm{Zero}_{\mathbf{R}}(PS) = \mathrm{Zero}_{\mathbf{R}}(CS), \tag{6.5.149}$$

其中 CS 由 (6.5.140) 和 (6.5.141) 给出.

证明 由前面引理，应该有 $f_{23} \neq 0, I_4 \neq 0$. 所以，定理可由 (6.5.143) 推出. □

Puma560 的值域和奇异性

我们只限于讨论智能 560 的一般性情形，即 (6.5.142) 中的任何初式均不为零. 由定理 6.5.35, 这是 $h_{42} * N_1 * N_2 \neq 0$ 的特殊情形. 在这种情形下，我们可由引理 6.5.30 直接得到下列引理和定理.

引理 6.5.36 在 (6.5.142) 中的任何初式均不为零的情况下， C_2, C_4, C_6 的判别式分别由下列式子给出：

$$\left.\begin{aligned} &D_2 = h_{41}^2 + h_{42}^2 - d_{23}^2 \geq 0,\\ &D_4 = 4 * a_2^2 * (d_4^2 + a_3^2) - (f_{43}^2 + f_{41}^2 - d_4^2 - a_3^2 - a_2^2) \geq 0,\\ &D_6 = (c_{23} * f_{31} + s_{23} * h_{33})^2 + f_{32}^2 \geq 0, \end{aligned}\right\} \tag{6.5.150}$$

其中 $(\varepsilon_2 = \pm 1)$,

$$\left.\begin{aligned} &f_{41} = \varepsilon_2 * D_2 - a_1,\\ &f_{31} = \frac{h_{41} * h_{32} - h_{42} * h_{31} * d_{23} + \varepsilon_2 * (h_{42} * h_{32} + h_{41} * h_{31}) * \sqrt{D_2}}{h_{41}^2 + h_{42}^2}. \end{aligned}\right\} \tag{6.5.151}$$

进一步地，利用 (6.5.145), (6.5.146), (6.5.150) 和 (6.5.151), 角 $\theta_1, \theta_{23}, \theta_4$ 将由 $C_2 = 0, C_4 = 0, C_6 = 0$ 来确定.

定理 6.5.37 当 $h_{42} * N_1 * N_2 \neq 0$ 时, Puma560 的值域部分可由下列式子给出：

$$\begin{aligned} &h_{41}^2 + h_{42}^2 \geq d_{23}^2,\\ &4 * a_2^2 * (d_4^2 + a_3^2) \geq (f_{43}^2 + f_{41}^2 - d_4^2 - a_3^2 - a_2^2)^2. \end{aligned}$$

对于上述值域中给定的手位置，有 8 个可能的控制参数集合；当上述不等式变成等式时，就会出现分支.

第七章　在几何定理证明中的应用

§7.1　几何定理机器证明的基本原理

记号 $\mathbf{K}, X = (x_1, \cdots, x_n)$ 等同前.

几何定理证明历史发展的回顾

我们在第 2 章中把几何定理证明的发展历史描叙成四个阶段. 从 Euclid 方式的第一阶段到 Descartes 方式的第二阶段的转折点出现在 17 世纪, 这是因为 Descartes 解析几何的出现. 这使基于公理化系统的逻辑演绎定理证明转向于基于坐标系统的代数计算定理证明. 可是, 从公理系统到坐标系统的跳跃不是平凡的. 是 Hilbert 第一次在他的经典著作《几何基础》中填补了中间的鸿沟, 如下:

$$\text{公理系统} \underset{(1)}{\longrightarrow} \text{数系统} \underset{(2)}{\longrightarrow} \text{坐标系统} \qquad (*)$$

而第 (2) 步在今天看起来很普通, 但第 (1) 步相当棘手. 我们下面更详细地讨论这一点.

Euclid 几何的 Hilbert 公理系统

我们限定于平面的情形. 为了建立 Euclid 几何的严格基础, Hilbert 把公理分成 5 类:

H-I. 关联公理 (Axioms of incidence).

H-II. 顺序公理 (Axioms of order).

H-III. 合同公理 (Axioms of congruence).

H-IV. 平行公理 (Axioms of parallels).

H-V. 连续公理 (Axioms of continuity).

正像 P. K. Rashevsky 在 Hilbert《几何基础》的俄文译版中的序言中指出, 关于连续性的第 5 类公理在 Euclid 几何的建立中实际上并没起到作用, 这个事实是几何定理证明机械化的重要基础. 另一方面, 另外四类公理是相互关联的. 例如顺序公理就被用来定义关联的概念. 在这样一个公理系统下, Hilbert 说明了如何引入一个实际上特征为零的域的数系统, 然后可以像上面表 (*) 那样在通常方式下引入坐标系统.

Desargues 定理和 Pascal 定理的作用

在 Hilbert 的经典著作中说明了有两个定理在数系统的引入中起到重要作

用，它们与以上面考虑的五类公理中的某些公理集所定义的几何有内在的联系．一个定理是如在第二章中例 2.1.5 描述的 Desargues 定理，而这个例子实际上是在现代术语所描述的一般的 Desargues 定理的一个特殊情形．Hilbert 说明了在没有合同公理而把 Desargues 定理作为一个公理的情况下，如何仍把一个数系统 (不必为特征零) 引入到几何系统中．此外，在这种公理体系下，平面几何可以扩充到一个空间几何，这说明 Desargues 定理的特殊几何意义．另一个扮演特殊作用的定理是 Pascal 定理，它实际是 Pappus 定理的一个特例．而在现代术语中 Pappus 定理反过来又是 Pascal 定理的特例．Hilbert 还说明了如果我们去掉合同公理，而把 Pascal 定理作为一个公理，那么引入的数系统遵守乘法交换律，且是一个特征为零的域．这就说明了 Pascal 定理或 Pascal 公理的特殊作用：它跟乘法交换性质有密切的联系．

Desargues 几何和 Pascal 几何

在作者写的 [WWT5] 一书中，我们提出了 Hilbert 公理系统的一个修改版．修改后的系统首先考虑包含关联公理和平行公理以及另外两个公理．一个是无穷公理以去除对应于通常有限几何的情形，另一个是 Desargues 公理，对应于例 2.1.3．我们省略细节 (可参考 [WWT5] 一书)，而引用下面的定义和定理．

定义 7.1.1　一个 Desargues 公理系统是指 H-I 公理，H-IV 公理，无穷公理和 Desargues 公理组成的公理系统．

定义 7.1.2　一个 (平面) 无序 Desargues 几何是指由符合 Desargues 公理系统的点和线所构成的几何．

定义 7.1.3　如果数系统有两个二元运算，+ 和 *，除了乘法交换律外，遵守通常的加法和乘法运算规则，并且有一个同构于通常的有理数集的子集，则称该数系统为一个 Desargues 数系统．

定理 7.1.4　对应一个 (平面) 无序 Desargues 几何，存在一个与之内在相关的 Desargues 数系统．

定理 7.1.5　在一个 (平面) 无序 Desargues 几何中，可以引入一个坐标系统，该几何的直线可由方程 $a*x+b*y=c$ 表示，其中 (x,y) 为坐标，a,b,c 属于某个内在的 Desargues 数系，且 a,b 不同时为零．

注释 7.1.6　在一个 (平面) 无序 Desargues 几何中，方程 $x*a+y*b=c$ 在一般情况下并不同于方程 $a*x+b*y=c$，也可以不是一条直线．

定义 7.1.7　一个 Pascal 公理系统是指由 H-I 公理，H-IV 公理，无穷公理

和 Desargues 公理，Pascal 公理组成的公理系统.

定义 7.1.8 一个 (平面) 无序 Pascal 几何是指满足 Pascal 公理系统的点和面所构成的几何.

定理 7.1.9 对于一个 (平面) 无序 Pascal 几何，存在一个与之内在相关的唯一的特征零的域.

定理 7.1.10 在一个 (平面) 无序 Pascal 几何，可以引入一个坐标系统，该几何的直线可由方程 $a * x + b * y = c$ 表示，其中 (x, y) 为坐标，a, b, c 属于某个内在的 Desargues 数系，且 a, b 不同时为零.

<u>度量几何、常用几何和欧几里得几何</u>

通过向 Pascal 公理系统中添加 Hilbert 公理系统中的公理，我们得到一系列几何系统. 下面将讨论其中一些最重要的系统.

定义 7.1.11 一个 (平面)*(无序) 度量几何* 是指由符合 Pascal 公理系统和 Hilbert 合同公理的点和直线的几何.

定义 7.1.12 一个 (平面)*常用几何* 是指由符合 Pascal 公理系统以及 Hilbert 合同公理和顺序公理的点和直线的几何.

定义 7.1.13 一个 (平面)*Euclid 几何* 是指由符合 Pascal 公理系统以及 Hilbert 合同公理、顺序公理和连续性公理的点和直线的几何.

<u>几何概念的代数化</u>

在所有上面的几何中，坐标系统可以被引入，从而各种几何体和几何关系可以用代数表达式或代数关系式的形式表示. 如果几何系统也满足 Pascal 公理，那么乘法是交换的，于是可以证明下面的定理是正确的.

定理 7.1.14 在无序 Pascal 几何和 Euclid 几何间的几何体系中，任何几何体可以表达成多项式的形式，任意几何关系可以表达为由逻辑符号 $\exists, \forall, \wedge, \vee, \neg$ 连接的多项式方程、多项式不等方程或者不等式.

注释 7.1.15 上面定理所引入的代数表达式和代数关系式可能相当复杂. 例如，令 $P_i = (a_i, b_i), i = 1, \cdots, 4$, 为使得直线 P_1P_2 和 P_3P_4 在通常意义下几何平行的四个点. 那么首先要使 P_1P_2 和 P_3P_4 成为实际上的几何直线，点 P_1, P_2 以及 P_3, P_4 应该是相异的. 代数上，这意味着下面的方程应被满足：

$$\neg(a_2 = a_1 \wedge b_2 = b_1), \quad \neg(a_4 = a_3 \wedge b_4 = b_3), \tag{7.1.1}$$

仅在这种情形下，两条几何直线 P_1P_2 和 P_3P_4 可以分别地由下面的方程所定义：

$$\begin{vmatrix} x & y & 1 \\ a_1 & b_1 & 1 \\ a_2 & b_2 & 1 \end{vmatrix} = 0, \quad \begin{vmatrix} x & y & 1 \\ a_3 & b_3 & 1 \\ a_4 & b_4 & 1 \end{vmatrix} = 0. \tag{7.1.2}$$

其次，对于在通常意义下几何平行的两条几何直线 P_1P_2, P_3P_4，它们应该互不相同，或者点 P_3, P_4 不在几何直线 P_1P_2 上. 代数上，我们应该有下面满足的不等方程，即

$$\begin{vmatrix} a_1 & b_1 & 1 \\ a_2 & b_2 & 1 \\ a_3 & b_3 & 1 \end{vmatrix} \neq 0, \quad \begin{vmatrix} a_1 & b_1 & 1 \\ a_2 & b_2 & 1 \\ a_4 & b_4 & 1 \end{vmatrix} \neq 0. \tag{7.1.3}$$

仅在这种情形下，两条不同的几何直线 P_1P_2, P_3P_4 的几何平行性可以在通常的几何意义下定义，可以变换成下面的代数关系式:

$$(a_2 - a_1) * (b_4 - b_3) - (a_4 - a_3) * (b_2 - b_1) = 0. \tag{7.1.4}$$

于是，通常几何意义上的两条直线平行就代数等价于一组方程和不等方程 (7.1.1)~(7.1.4). 如果都是用这种方式把几何概念转换为代数表达式和代数关系式，那么用代数手段来研究几何问题将很困难. 为了避免这种不合需要的复杂性，我们采用下面的措施.

我们称 (7.1.2) 中的第一个方程表示连接两个点 P_1 和 P_2 的直线，不论 P_1, P_2 是否不同或者不论 (7.1.1) 中相应的不等方程是否满足. 在前者 P_1P_2 为一条普通 *几何* 直线，而在后者我们称 P_1P_2 为一条 *退化* 直线或者 *在退化意义上* 的直线. 因此一条 *退化* 直线可以是整个平面上所有点的集合. 此外，当 (7.1.4) 成立时，我们称方程 (7.1.2) 表示的两条直线 P_1P_2 和 P_3P_4 是 *代数* 平行的. 只有在 (7.1.1) 和 (7.1.3) 满足时，P_1P_2 和 P_3P_4 表示两条互不相同的直线，而在 (7.1.4) 成立时是通常意义的 *几何* 平行直线. 另一方面，我们看到如果有一条或两条是 *退化* 的，或者当都非退化时两条直线重合，两条 *代数* 直线可以是 *代数* 平行的. 在这种情形下，我们称两条代数直线为 *退化* 平行的或者 *在退化意义上* 平行的.

为简单起见，我们不说一条 *代数* 直线或者两条 *代数* 直线是 *代数* 平行的，而去掉修饰词 *代数*，直接说一条直线或者两条直线是平行的. 对于 *非退化* 直线或者 *非退化* 平行直线，相应的代数关系式 (7.1.1) 或 (7.1.3) 称为 *非退化条件*. 其他的 *退化* 情形的 *代数* 几何体和关系可以用相似的方式引入. 在下面的讨论中，几何体和关系可以按照在前面的方式在代数意义上来理解.

关于几何定理退化的一些注记

在通常的几何定理中，几何体和几何关系是从通常适合的几何意义上理解，于是退化情形都是被隐含地舍弃掉的. 否则定理可能不成立，甚至失去本来的意义.

例 7.1.16 (定理) 对于一个平行四边形 $ABCD$, 两条对角线 AC 和 BD 相交于它们的公共中点 (或者有一个公共中点).

为了使这个定理为真，需要隐含地假定四条边 AB, BC, CD, DA 都为真正的几何直线，或者任一点对 A,B; B,C; C,D; D,A 都不重合. 更进一步，也隐含的假定两对对边为真正的几何直线，在通常的几何意义上互相平行. 事实上，如果这些隐含的假定不保留，定理可能不真，甚至失去意义. 例如，如果四条边为真正的几何直线，但边 AB, CD 仅相互退化平行，以致 AB, CD 退化成同一条直线，C, D 在直线 AB 上，那么 AC 和 BD 的中点通常不再是同一个点. 此外，相交也失去了其意义.

例 7.1.17 让我们再考虑第二章中的例 2.1.5. 我们已经看到对于这里考虑的情形，如果两个三角形 ABC, $A'B'C'$ 的对应边 BC, $B'C'$ 是退化平行的，定理将不再成立. 相似地，如果三角形 $ABC, A'B'C'$ 是退化的，于是它们不再是通常意义上真正的三角形，而是退化为直线，则第二章中的例 2.1.5 中的 Desargues 定理的逆命题不再成立. 参看下面的附图 7.1. 也可参照第二章中的图 2.4~2.6 和第三章中的图 3.6.

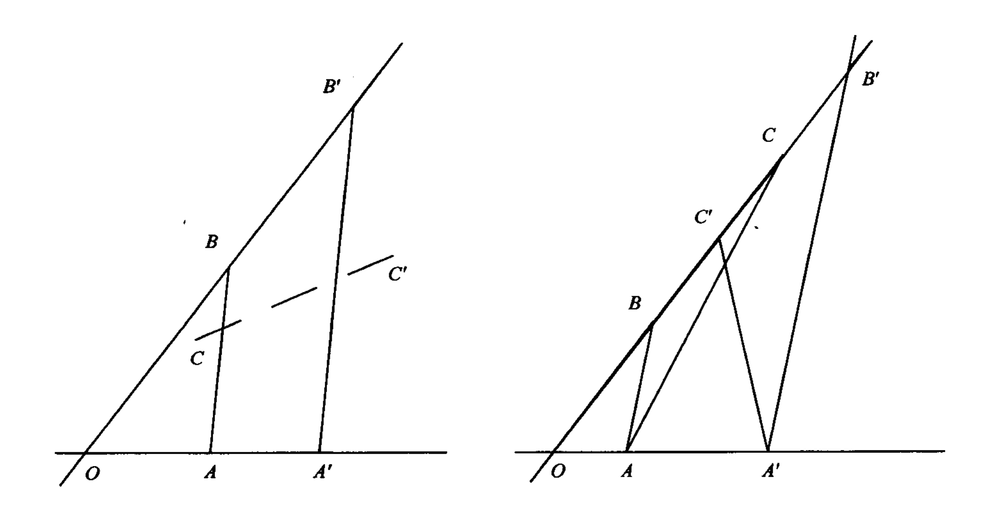


图 7.1 Desargues 定理的逆命题不成立的情形

初等几何的概念

在一定意义上说，上面所描述的几何 (平面的或空间的) 都附属于常用几何或 Euclid 几何. 然而有很多种几何并不具有这种特性，例如射影几何，线几何，非欧几何，圆几何等等. 在 [WWT5] 中，介绍了如何在公理系统的基础上定义这些几何，如何像常用几何或者附属于常用几何的几何那样引入数系统和一个坐标系统. 它也说明了对于上面的几何，与这些几何内在关联的的数系统实际上是特征为零的域. 至今，类似于前面在 Hilbert 公理体系中引入了 Pascal 定理已被引入到相关的几何公理系统定义中，则对于这些几何我们可以引入坐标系统及几何概念的代数化，然后不必参考原来基本的公理系统，而在 Descartes 的方式下处理几何定理证明. 我们甚至可以采取下面极端的处理：

我们将彻底放弃基于公理系统几何的 Euclid 方式. 相反地，我们将在 Descartes 几何方式下直接从数系统和坐标系统来处理这些几何. 事实上，我们在几何的数学研究中已经遵循这种处理方式. 因此，为了研究平面射影几何我们从实数或复数域开始，然后引入齐次坐标，以三元组 $(a:b:c)$ 的比率表示一个点，其中 a,b,c 为域中不全为零的数. 然后通过代数方程或表达式，我们可以定义直线、点的共线、直线上四个点的交比，等等. 然后通过代数表达式或方程的代数处理来研究射影几何. 用相同的方式，我们可以不必参照可能的基本公理系统来研究各种几何. 如果我们按照 Klein 的观点来看几何，公理系统的记号明显是根本多余的. 我们进一步考虑微分几何的情形. 对于三维的情形，我们通常用在坐标系统下满足某些可微性和正则性条件的一个方程或一对方程来定义一个 *曲面* 或一条 *曲线*. 我们也可以用参数方程以相同的方式来定义. 在任何情况下，我们将直接从这些方程来定义这些曲线或曲面的有几何意义的性质. 于是我们可以通过纯代数或微分的手段来研究做曲线和曲面的几何. 这里没有涉及到任何公理系统. 事实上，对于这种微分几何，作者忽略了任何公理系统. 甚至引入这样一个公理系统的可能性看起来也值得怀疑.

为此，我们将直接从一个数域 (主要是特征零的域) 和这个域中的坐标系统开始研究几何，而不去考虑式 (*) 的第 (1) 步和第 (2) 步.

对于微分几何，某些微分运算应该从基域中引入. 在本书中我们仅限于讨论不包含微分的几何. 我们将模糊地称这样的几何为初等几何，以区别于通常意义上的微分几何.

初等几何中的几何定理和几何定理证明

现在我们考虑任何上面所描述的基本几何. 我们假定基域或者与这个几何

内在相关的数域是一个特征为零的域 $\mathbf{K}$, 坐标系统为 $X=(x_1,\cdots,x_n)$. 我们进一步假定几何体或者几何关系式可以表达成 $\mathbf{K}[X]$ 中多项式的形式. 那么, 几何定理一般可以写成形式 $T=\{H_T,C_T\}$, 其中 H_T 表示由 $\exists,\forall,\wedge,\vee,\neg$ 所连接的多项式或者有理方程, 不等方程, 或者不等式形式的假设条件. 相似地, 可以表示结论部分 C_T. 在任何情形下, 本书中仅考虑可以写成这种形式的几何定理. 在这种理解下, 所有这样的定理的域将像下面所定义的一样记作 $\mathbf{T}$:

定义 7.1.18 几何定理的 Tarski范围 是指形如 $T=\{H_T,C_T\}$ 的几何定理的范围, 其中 H_T 指 假设, C_T 指 结论, 两者都是由逻辑符连接的多项式或者有理方程、不等方程、或者不等式集合的形式.

定理 7.1.19 (Tarski 定理) 存在一个算法, 允许我们在有限步内决定范围 $\mathbf{T}$ 中的一个定理 $T=\{H_T,C_T\}$ 是否正确, 或者说 C_T 是否是 H_T 的结论.

注释 7.1.20 并非所有的通常的常用几何中的著名定理都属于域 $\mathbf{T}$. 例如, Jordan 定理断言任意的平面简单闭多边形把平面分成两个部分, 这就不属于 $\mathbf{T}$.

特殊情形: 范围 $\mathbf{H}$ 和 $\mathbf{E}$

定义 7.1.21 几何定理的 Hilbert范围$\mathbf{H}$ 是指定理 $T=\{HYP,CONC\}$ 的范围, 其中 $HYP=\{P_1,\cdots,P_r\}$, $P_k=x_k-R_k, R_k\in\mathbf{K}(X_{k-1},U), CONC\in\mathbf{K}(X,U)$, U 为有限参数集. 定理 T 的假设和结论分别为 $HYP=0$ 和 $CONC=0$.

定义 7.1.22 几何定理的 相等范围$\mathbf{E}$ 是指定理 $T=\{HYP,CONC\}$ 的范围, 其中 $HYP\subset\mathbf{K}[X]$ 且 $CONC\in\mathbf{K}[X]$. 定理 T 的假设和结论分别为 $HYP=0$ 和 $CONC=0$.

我们将在下一节中研究范围 $\mathbf{H}$ 中的几何定理证明. 下面我们列出在范围 $\mathbf{E}$ 中定理证明的一些基本原理, 而把实际的定理证明放在第 7.3 节.

$\mathbf{E}$ 中定理证明的基本原理

在 Zero(HYP) 中的每一个零点 X^0 满足定理 T 中的假设, 也是扩张空间 $\mathbf{K}'^n$ 中的一个几何构型, 其中 $\mathbf{K}'$ 为 $\mathbf{K}$ 的扩域. 对于这样一个几何构型, 如果 $CONC$ 在该几何构型相对应零点 X^0 处为零, 则结论是正确的. 于是要证明一个几何定理, 就等于寻找 Zero(HYP) 的一个有意义的部分 P, 使得在 P 上有 $CONC=0$ 成立. 关于 Zero(HYP) 的零点结构的一些定理将给我们提供寻找这样的 P, 以及在 P 上验证 $CONC=0$ 的方法.

整序原理 $\Longrightarrow$

机械化几何定理证明原理 I. 对于范围 $\mathbf{E}$ 中的一个给定的定理 $T = \{HYP, CONC\}$, 设 CS 为假设多项式集 HYP 的一个特征列, IP 为 CS 的初式乘积, 那么

$$\text{Remdr}(CONC/CS) = 0 \tag{7.1.5}$$

是下式的一个充分条件:

$$\text{Zero}(HYP/IP) \subset \text{Zero}(CONC). \tag{7.1.6}$$

也就是说 (7.1.5) 是定理 T 在

$$IP \neq 0 \tag{7.1.7}$$

成立的一个充分条件. 进而, 如果 CS 是一个不可约升列, 条件 (7.1.5) 也是定理 T 成立的必要条件.

证明 我们令

$$R = \text{Remdr}(CONC/CS). \tag{7.1.8}$$

由第三章中的余式公式 (3.3.27), 对于某些多项式 Q_i 和 CS 中多项式 C_i 的初式幂积 I_{CONC}, 我们有下面形式的公式:

$$I_{CONC} * CONC = \sum_i Q_i * C_i + R. \tag{7.1.9}$$

由第 3 章的良序原理 (定理 3.3.37) 我们也有

$$\text{Zero}(CS/IP) = \text{Zero}(HYP/IP) \subset \text{Zero}(HYP) \subset \text{Zero}(CS). \tag{7.1.10}$$

我们首先假定 $R = 0$. 考虑满足问题假设的任一几何构型, 例如 HYP 的某一零点 X^0. 由 (7.1.10) 的第二部分, X^0 也是所有多项式 C_i 的零点. 如果 X^0 不是 IP 或者 C_i 的任一初式的零点, 那么 X^0 就不是 I_{CONC} 的一个零点. 从而由 (7.1.9) 和 $R = 0$ 可知, X^0 是 $CONC$ 的一个零点, 即 (7.1.6) 成立. 这就证明了原理的第一部分.

假定 CS 不可约, 且 (7.1.6) 成立. 于是, 对于任何一个使 CS 的任何初式不为零的点 $X = X^0$ 对应的几何构形, 定理 T 为真. 特别地, 如果 $X = \Xi^0$ 是由不可约升列 CS 所定义的母点, 那么由定理 (3.6.7), 在 Ξ^0 上 CS 的任何初式不为零, 所以 $\Xi^0 \in \text{Zero}(CS/IP) = \text{Zero}(HYP/IP)$. 这个 Ξ^0 必是所有多

项式 C_i 的一个零点，又由假定 (7.1.6) 可知它也是 $CONC$ 的一个零点. 于是由 (7.1.9), Ξ^0 为 R 的一个零点. 由于 R 相对于不可约升列 CS 是约化的，我们由定理 (3.6.7) 得到 $R=0$. 这就证明了原理的第二部分. □

零点分解定理 $\Longrightarrow$

机械化几何定理证明原理 II 对于范围 $\mathbf{E}$ 中任一给定的定理 $T = \{HYP, CONC\}$, 设 AS_i 为由满足下式的假设多项式集 HYP 所决定的升列的一个集合，

$$\text{Zero}(HYP) = \bigcup_i \text{Zero}(AS_i/IP_i), \tag{7.1.11}$$

其中 IP_i 为相应的升列 AS_i 的初式乘积. 如果

$$\text{Remdr}(CONC/AS_i) = 0, \tag{7.1.12}$$

那么定理 T 在 $\text{Zero}(HYP)$ 的 $\text{Zero}(AS_i/IP_i)$ 部分上成立，或者

$$\text{Zero}(AS_i/IP_i) \subset \text{Zero}(CONC). \tag{7.1.13}$$

反之，如果 AS_i 不可约且定理 T 在 $\text{Zero}(HYP)$ 的 $\text{Zero}(AS_i/IP_i)$ 部分为真，或者 (7.1.13) 成立，则我们有 (7.1.12).

证明 与原理 I 的证明类似，只需用 AS_i 来代替 CS. □

簇分解定理 $\Longrightarrow$

机械化几何定理证明原理 III 对于域 $\mathbf{E}$ 中一个给定定理 $T = \{HYP, CONC\}$, 设 IRR_k 为由满足下式的假设多项式 HYP 所决定的不可约升列的一个集合：

$$\text{Zero}(HYP) = \bigcup_k \text{Var}[IRR_k], \tag{7.1.14}$$

那么在不可约分支 $\text{Var}[IRR_k]$ 上定理 T 为真，当且仅当

$$\text{Remdr}(CONC/IRR_k) = 0. \tag{7.1.15}$$

证明 由机械化几何定理证明原理 II, (7.1.15) 成立当且仅当

$$\text{Zero}(IRR_k/IP_k) \subset \text{Zero}(CONC), \tag{7.1.16}$$

其中 IP_k 为不可约升列 IRR_k 的初式乘积. 根据 (3.6.124), 我们有

$$\text{Zero}(IRR_k/IP_k) \subset \text{Var}[IRR_k]. \tag{7.1.17}$$

于是从

$$\mathrm{Var}[IRR_k] \subset \mathrm{Zero}(CONC) \tag{7.1.18}$$

可以得出 (7.1.16) 和 (7.1.15). 反之, 假定 (7.1.15) 成立, 所以 (7.1.16) 也成立, 或者定理 T 在 $\mathrm{Zero}(IRR_k/IP_k)$ 部分上成立. 设 Ξ_k 为 $\mathrm{Var}[IRR_k]$ 的一个母点. 那么由定理 (3.6.6) 我们有

$$\Xi_k \in \mathrm{Zero}(IRR_k/IP_k). \tag{7.1.19}$$

于是, 从 (7.1.16) 可以得出 $\Xi_k \in \mathrm{Zero}(CONC)$. 由于 $\mathrm{Var}[IRR_k]$ 的所有点是 Ξ_k 在 $\mathbf{K}$ 上的特定化, 我们有 (7.1.18) 成立. 因此, (7.1.18) 等价于 (7.1.16), 即 (7.1.15). □

一些注释

注释 7.1.23 从机械化几何定理证明原理 I 我们看到 (7.1.7) 实际上给出了在问题 $T = \{HYP, CONC\}$ 中如果 (7.1.5) 满足时定理为真的非退化条件. 在那种情形下, 我们称定理 T 在非退化条件 (7.1.7) 下 一般 正确.

注释 7.1.24 对于范围 **E** 中的定理, 机械化几何定理证明原理 I~III 给出了几何定理证明的三种不同方法. 原理 I 是最简单的方法, 但要在一般意义上证明定理时是不完备的, 因为定理仅在一般意义下证明. 在原理 III 中的方法是最完备的方法, 没有引入退化条件, 但应用起来很困难.

注释 7.1.25 对于含有不等式的范围 **T**, Tarski 算法是非常复杂的, 甚至难于证明任何一个有趣的定理. 然而, 我们在后面将会考虑用一些完全不同的方法来处理一些特殊情形, 这些方法是可行的和有效的.

注释 7.1.26 在后面的章节里, 我们将给出具体的例子来描述几何定理证明的不同方法.

注释 7.1.27 本书中我们将限于讨论基域为特征零的情形. 可是, 就定理证明而言, 对于在基域特征为正素数的有限几何中的定理证明本身是很有趣的. 尽管在此我们不做过多的介绍, 读者可参考 Lin 和 Liu 的一些有趣的原始文章, 例如 [L-L1,2]. 也可看本书 §8.5 中的一些段落.

§7.2　Hilbert 型几何定理的机器证明

下面我们将假设与几何数系内在相关联的数系是特征为零的域. 通常为有理数域 **Q**. 我们把该域记为 **K**, 也沿用前面章节的记号.

显式构造性与 Hilbert 型定理

沿着 7.1 节中描述几何定理证明的一般思路，我们采用某个坐标系统，把几何实体和几何关系转化成按通常序排列的变量 $X=(x_1,\cdots,x_n)$ 之间的代数表示，它们可以是点的坐标、直线方程的系数、比率、距离等.

定义 7.2.1 一个几何实体可以从一些已经构造的几何实体显式地构造当且仅当出现该几何实体中的变量属于有理函数域 $\mathbf{K}(X')$, 其中 X' 代表出现在已经构造的几何实体中的变量和新引进的参数.

定义 7.2.2 一个几何定理是 显式构造型的 或 Hilbert型 当且仅当定理中涉及的几何实体可以通过由任意参数确定的几何实体和已经显式地构造出的几何实体逐个引入.

Hilbert 机械化定理

作为上述定义的一个结论，对于一个 Hilbert 型或属于范围 $\mathbf{H}$ 中的几何定理 $T=\{HYP,CONC\}$, 涉及几何对象的相应变量可以按确定的序排列，即

$$x_1 \prec x_2 \prec \cdots \prec x_n,$$

使得对于假设条件我们有

$$x_{i_k}=\frac{P_{i_k}}{Q_{i_k}},\ P_{i_k},Q_{i_k}\in \mathbf{K}[X_{i_k-1}], \tag{7.2.20}$$

其中 i_k 取遍子集 $N'=\{i_1,\cdots,i_r\}\subset N=\{1,2,\cdots,n\}$ 且 $i_1<\cdots<i_r$. 方程 (7.2.20) 组成了包含有理函数 $x_{i_k}=\frac{P_{i_k}}{Q_{i_k}}$ 的假设集 HYP. 参见定义 7.1.21. 为了验证定理是否正确，只需要根据方程 (7.2.20), 按照逆序逐次消去变元 x_{i_k} 即可. 准确地说，令 U 为包含变量 x_i 的集合，其中 $i\in N\setminus N'$. 当 $s>0$ 时，$X_s^+=U+X_s$, 构造下面的过程:

$$\begin{aligned} CONC = R_r(X) &\underset{(r)}{\longrightarrow} R_{r-1}(X^+_{i_r-1}) \underset{(r-1)}{\longrightarrow}\cdots\underset{(1)}{\longrightarrow} R_0(X^+_{i_1-1})\\ &= R_0(U). \end{aligned} \tag{*}$$

在 (*) 中，每一步骤 (k) 包含 R_k 中用 (7.2.20) 的 $\frac{P_{i_k}}{Q_{i_k}}$ 代替 x_{i_k}. 于是讨论中的定理 一般是正确的 当且仅当消元的最后结果 R_0 等于 0. 这里一般是正确的是指定理在非退化条件 $Q_0\neq 0$ 与 $Q_{i_k}\neq 0(i_k\in N')$ 下是正确的，其中 Q_0 是 $CONC$ 的分母.

为了便于计算，我们也可以把方案 (*) 修改为下面的 (**):

$$CONC = R_r(X) \underset{(r)}{\longrightarrow} N_{r-1}(X^+_{i_r-1}) \underset{(r-1)}{\longrightarrow}\cdots\underset{(1)}{\longrightarrow} N_0(X^+_{i_1-1})$$

$$= N_0(U). \tag{**}$$

在 (**) 中, 每一个 N_k 是在上一步 N_{k+1} 中用 (7.2.20) 中的 $\frac{P_{i_k}}{Q_{i_k}}$ 代替 x_{i_k} 得到的有理函数的分子, N_r 是 $CONC = R_r(X)$ 分子. 作为另一种方法, 我们也可以借助于 $(7.2.20)_j$, $j < k$, 先把每一个方程 $(7.2.20)_k$ 约化为下面的形式:

$$x_{i_k} = \frac{P'_{i_k}}{Q'_{i_k}},\ P'_{i_k}, Q'_{i_k} \in \mathbf{K}[U], \tag{7.2.21}$$

然后再利用 (*) 或 (**).

由于方法 (*) 与 (**) 是机械化的, 我们可以得到下面的定理. 也可以参见第 2.2 节.

定理 7.2.3 (Hilbert 机械化定理) Hilbert 型几何定理或者范围 **H** 中的定理是可以机械化的.

<u>显式可构造性的例子</u>

根据 Hilbert 的原始陈述, 可以显式构造仅仅局限于两直线相交, 两直线平行与点共线, 一句话, 就是线性型的构造. D. M. Wang 首先指出 Hilbert 显式构造性的思想的适用范围可以极大地推广, 而不仅仅局限于线性特征的几何构造, 例如推广到正交. 另外, X. S. Gao, X. L. Lue 等人进一步地推广了这些可以显式构造的范围. 下面是一些局限于常用几何的例子. 普通平面或者空间的坐标系统分别为 (Y_1, Y_2) 和 (Y_1, Y_2, Y_3).

构造 2.1 两条直线的交点是可以显式构造的. 类似地, 连接两点的直线是可以显式构造的.

事实上, 令两条给定的直线有下面的形式:

$$\begin{aligned} L_1&: u_1 * Y_1 + u_2 * Y_2 = u_3, \\ L_2&: u_4 * Y_1 + u_5 * Y_2 = u_6, \end{aligned} \tag{7.2.22}$$

其中 u_i 是新参数或是已经引入的变量. 交点 (z_1, z_2) 由

$$z_1 = \frac{u_3 * u_5 - u_6 * u_2}{u_1 * u_5 - u_2 * u_4},\ z_2 = \frac{u_1 * u_6 - u_3 * u_4}{u_1 * u_5 - u_2 * u_4} \tag{7.2.23}$$

给出. 这些方程说明交点是可以显式构造的. 非退化条件由

$$u_1 * u_5 - u_2 * u_4 \neq 0 \tag{7.2.24}$$

给出. 其意义是两条直线不是 (代数) 平行的. 类似地, 对于给定的两个点 $P_1 = (u_1, u_2), P_2 = (u_3, u_4)$, 直线 P_1P_2 由

$$z_1 * Y_1 + z_2 * Y_2 + z_3 = 0$$

给出，其中

$$z_1 = u_2 - u_4,\ z_2 = u_3 - u_1,\ z_3 = u_1 * u_4 - u_2 * u_3. \tag{7.2.25}$$

非退化条件为

$$u_2 \neq u_4, \quad \text{或 } u_1 \neq u_3. \tag{7.2.26}$$

构造 2.2 两点间距离的平方是可以显式构造的，但是距离本身却不可以. 对于给定两个点 $(u_1, u_2), (u_3, u_4)$, 它的距离平方 $(u_3 - u_1)^2 + (u_4 - u_2)^2$ 是可以显式构造的. 另一方面距离本身不能表示为 u_i 的有理函数，从而是不能显式构造的.

我们在下面列出一些可以显式构造的例子以供参考，其中表示新变量的方程可以很容易地根据已知变量来确定.

构造 2.3 一点到一条直线的垂足是可以显式构造的，但是垂线的长度却并不然.

构造 2.4 一点或一条直线相对于一条直线的反射是可以显式构造的，但是一个角的平分线并不然.

构造 2.5 一条过圆上一点的直线与这圆的另一交点是可以显式构造的，但是一条直线与一个圆的交点并不是可以显式构造的.

构造 2.6 三角形的外接圆圆心是可以显式构造的，但是三角形的内心或旁心却不是可以显式构造的. 外接圆的半径以及内切圆或旁切圆的半径都是不可以显式构造的. 普通空间中球面外接或者内切于一个四面体的情形类似.

构造 2.7 过不在圆上的一点的圆的切线不是可以显式构造的，但是过圆上一点的圆的切线是可以显式构造的.

可以显式构造和不可以显式构造的几何实体的表几乎可以无穷地增加，特别是当考察的几何超出初等几何或者 Euclid 几何的范畴.

Hilbert 型定理的示例

尽管 Hilbert 最初考虑的是具有线性特征的可以显式构造的几何定理，但是它已经包含了很多非平凡的有趣的定理. 作为例子，我们将要指出，除了 Pappus 线定理与 Pascal 线定理，以及在两条直线上的点的三元组的 Pappus 线定理，与 Pascal 二次曲线定理，其他都是本文作者发现和证明的. 在前面的构造中，可以显式构造的类型已经拓广. 为说明这一点，下面我们给出一些涉及圆或者度量性质的定理，所有的这些定理都具有 *非线性* 特征，并且最初很难看出它们是可以显式构造的. 为了使定理是可以显式构造的，我们对每一

个定理的几何对象都按照一定的顺序进行了仔细排序.

例 7.2.4 (Simson 线定理)　设 D 为三角形 ABC 的外接圆上一点, 则从 D 到边 AB, AC, BC 的垂足 E, F, G 共线.

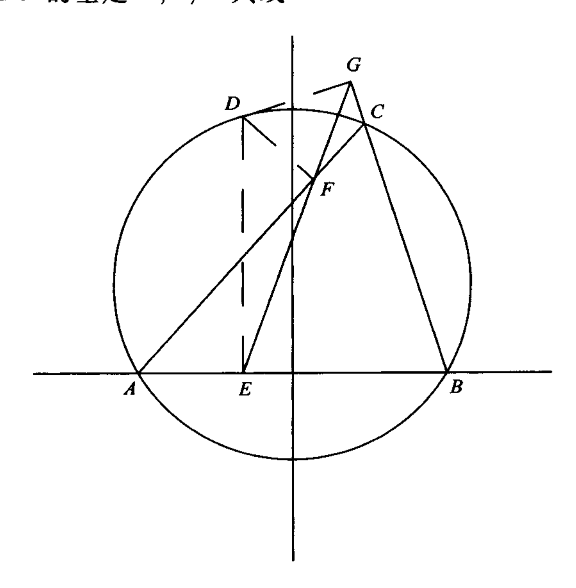


图 7.2　Hilbert 型定理的示例

证明　为说明本定理是 Hilbert 型的, 我们先进行坐标选取, 使得 A, B 与三角形 ABC 外接圆的圆心 O 为 $A=(x_1,0)$, $B=(-x_1,0)$, $O=(0,x_2)$. 为确定 C, D, 直线 AC, AD 为

$$\begin{aligned} AC:&\quad x_4 * (Y_1 - x_1) = x_5 * Y_2,\\ AD:&\quad x_8 * (X - x_1) = x_9 * Y. \end{aligned}$$

其中 x_4, x_5, x_8, x_9 为任意参数. 由构造 2.5 知, $C=(x_6,x_7), D=(x_{10},x_{11})$ 是可以显式构造的, 其中

$$x_6 = \frac{x_1 * (x_4^2 - x_5^2) + 2 * x_2 * x_4 * x_5}{x_4^2 + x_5^2},\quad x_7 = \frac{2 * x_4 * (x_2 * x_4 - x_1 * x_5)}{x_4^2 + x_5^2}, \tag{7.2.27}$$

$$x_{10} = \frac{x_1 * (x_8^2 - x_9^2) + 2 * x_2 * x_8 * x_9}{x_8^2 + x_9^2},\quad x_{11} = \frac{2 * x_8 * (x_2 * x_8 - x_1 * x_9)}{x_8^2 + x_9^2}. \tag{7.2.28}$$

最后由构造 2.3 知，垂线的垂足 $G=(x_{12},x_{13})$，$F=(x_{14},x_{15})$，$E=(x_{16},x_{17})$ 都是可以显式构造的，其坐标由下面给出：

$$\left.\begin{aligned} x_{12}&=\frac{x_{10}*(x_6+x_1)^2+x_7*x_{11}*(x_6+x_1)-x_1*x_7^2}{(x_6+x_1)^2+x_7^2},\\ x_{13}&=\frac{x_7*((x_6+x_1)*(x_{10}+x_1)+x_{11})}{(x_6+x_1)^2+x_7^2},\end{aligned}\right\}\tag{7.2.29}$$

$$\left.\begin{aligned} x_{14}&=\frac{x_1*x_4^2+x_4*x_5*x_{11}+x_{10}*x_5^2}{x_4^2+x_5^2},\\ x_{15}&=\frac{x_4*(-x_1*x_5+x_4*x_{11}+x_{10}*x_5)}{x_4^2+x_5^2},\end{aligned}\right\}\tag{7.2.30}$$

$$x_{16}=x_{10},\quad x_{17}=0.\tag{7.2.31}$$

对应于方程 (7.2.27)~(7.2.31) 的有理函数组成了假设集合 HYP. 结论 E,F,G 共线等价于

$$CONC\equiv\begin{vmatrix} x_{12} & x_{13} & 1\\ x_{14} & x_{15} & 1\\ x_{16} & x_{17} & 1\end{vmatrix}=0.\tag{7.2.32}$$

$CONC=0$ 的证明可以借助于 (7.2.31),(7.2.30), (7.2.29),(7.2.28),(7.2.27) 相继地把 x_{17}，x_{16}，x_{15}，x_{14}，x_{13}，x_{12}，x_{11}，x_{10}，x_7，x_6 消去. 与方案 (**) 一致，多项式 N_k 的相继指标集为

$$\begin{gathered} CONC:[6\ x_{17}\ 1]\longrightarrow[4\ x_{15}\ 1]\longrightarrow[9\ x_{13}\ 1]\longrightarrow[12\ x_{11}\ 2]\longrightarrow\\ [12\ x_9\ 1]\longrightarrow 0.\end{gathered}$$

从而该定理在非退化条件

$$x_4^2+x_5^2\neq 0,\quad x_8^2+x_9^2\neq 0,\quad (x_6+x_1)^2+x_7^2\neq 0$$

下 一般 正确. 该条件说明，当域 $\mathbf{K}$ 是实数域时，直线 AC,AD 是真正的几何直线并且 C 是不与 B 重合的点. □

例 7.2.5 (Feuerbach 定理 (1822)) 三角形的九点圆与它的内切圆和 3 个旁切圆相切.

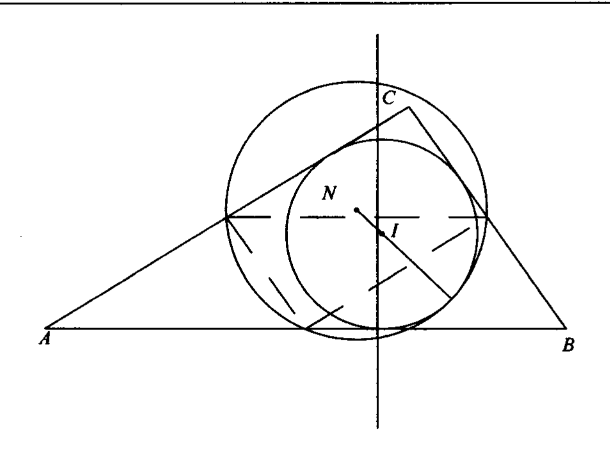


图 7.3 Feuerbach 定理

证明 为了使定理是可以显式构造型的，我们首先选取坐标系并适当地安排几何对象，使得三角形 ABC 的顶点和中心 I，不论是内心还是任何一个旁心，都由 $I=(0,x_1)$，$A=(x_2,0)$，$B=(x_3,0)$，$C=(x_4,x_5)$ 给出．由构造 2.4，直线 AC,BC 是 AB 分别相对于 AI,BI 的反射，它们都是可以显式构造的，于是它们的交点 C 也是可以显式构造的．由构造 2.1 知，C 的坐标 (x_4,x_5) 为

$$x_4=\frac{x_1^2*(x_2+x_3)}{x_1^2+x_2*x_3},\quad x_5=\frac{2*x_1*x_2*x_3}{x_1^2+x_2*x_3}. \tag{7.2.33}$$

于是边 AB,AC,BC 的中点显然是可以显式构造的．由构造 2.6 知，中点三角形的外心，即九点圆的圆心 $N=(x_6,x_7)$ 也是可以显式构造的，并且坐标 x_6,x_7 由

$$\begin{aligned} x_6 &= \frac{x_2+x_3+2*x_4}{4}, \\ x_7 &= \frac{x_5^2+(x_3-x_4)*(4*x_6-2*x_2-x_3-x_4)}{4*x_5} \end{aligned} \tag{7.2.34}$$

给出．由构造 2.2 可知，九点圆的半径的平方 x_8 和从九点圆到内切或者外接圆的距离的平方 x_9 都是可以显式构造的，其中

$$x_8=x_7^2+\left(x_6-\frac{x_2+x_3}{2}\right)^2,\quad x_9=(x_7-x_1)^2+x_6^2. \tag{7.2.35}$$

在不考虑圆的相切方式的情况下，结论等价于

$$CONC \equiv x_9^2+x_8^2-2*x_9*x_8-2*x_9*x_1^2-2*x_8*x_1^2+x_1^4=0. \tag{7.2.36}$$

不考虑 I 是内心还是旁心，也不考虑定理断言的相切的方式是内切还是外切，借助于根据方案 (**) 制定的证明步骤，只需要简单的验证 (2.14) 就可以看到结论是正确的. 相继的指标集如下：

$$CONC\colon [6\ x_9\ 2] \longrightarrow [11\ x_8\ 2] \longrightarrow [23\ x_7\ 1] \longrightarrow [45\ x_6\ 2] \longrightarrow$$
$$[18\ x_5\ 1] \longrightarrow [24\ x_4\ 3] \longrightarrow 0.$$

立即可以得出非退化条件为

$$x_1^2 + x_2 * x_3 \neq 0, \quad x_5 \neq 0.$$

$x_1^2 + x_2 * x_3 \neq 0$ 的几何意义是 AC 与 BC 不平行. $x_5 \neq 0$ 意味着 C 不在边 AB 上. 于是两个非退化条件都是平凡的. □

<u>包含角度的显式构造</u>

在 Euclid 的《几何原本》第三卷中，命题 21, 22 断言：对于在同一个圆上的两两不同的四个点 $A, B, C, D, \angle ACB$ 与 $\angle ADB$ 或者相等或者两两互补. 在 Euclid 风格中的几何定理的证明中，这种不明确性引起很多的麻烦：每次应用该命题的时候，我们不得不验证两个角是在同一个弧上还是在相对的弧上. 这是一个并不容易确定的事实. 为了避免这些麻烦，我们引入下面的概念：*定向角*.

定义 7.2.6 给定普通平面上两条实在的几何直线 L_1, L_2. 从 L_1 到 L_2 的 *定向角* 是指如果 L_1, L_2 相交，从 L_1 关于交点逆时针方向旋转到 L_2 的角 mod π. 否则定义为 0 mod π.

记号 7.2.7 从 L_1 到 L_2 的定向角记为 $< (L_1, L_2) = - < (L_2, L_1)$.

注释 7.2.8 定向角是在相差 π 的倍数的意义下定义的. 因此，其正切值是唯一确定的.

注释 7.2.9 为避免角的正切值可能是无穷大，我们将把正切表示成比率 $t_1 : t_2$ 的形式. 普通平面上直线的 *斜率* 通常是从水平轴到该直线的定向角的正切，我们也将之表示为比率的形式.

命题 7.2.10 对于在普通平面上处于任意位置的三条真实的几何直线 L_1, L_2, L_3, 我们有 $< (L_1, L_3) = < (L_1, L_2) + < (L_2, L_3)$.

注释 7.2.11 除非另外声明，上述等式以及后面类似的等式都被理解为是 mod π 同余的.

于是, Euclid《*几何原本*》中的命题 21, 22 现在可以被统一成下面的一个命题：

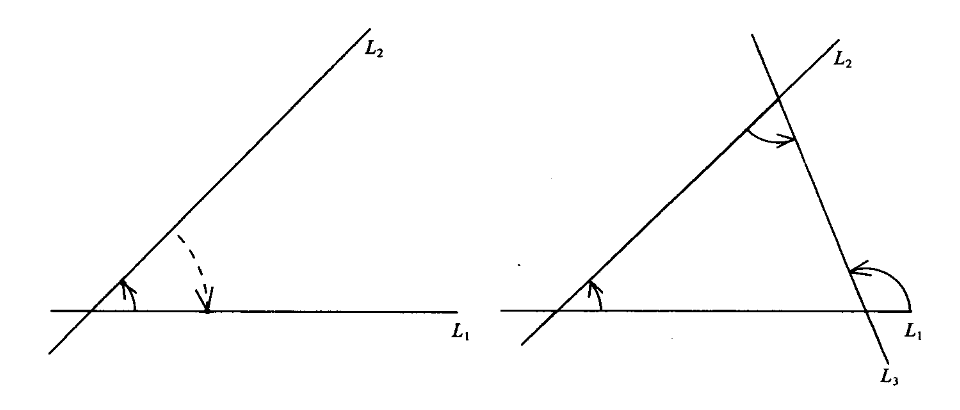


图 7.4　命题 7.2.10 的示意图

命题 7.2.12　在普通平面上，两两不重合的和不共线的四个点 A, B, C, D 共圆当且仅当 $<(AC, BC) = <(AD, BD)$.

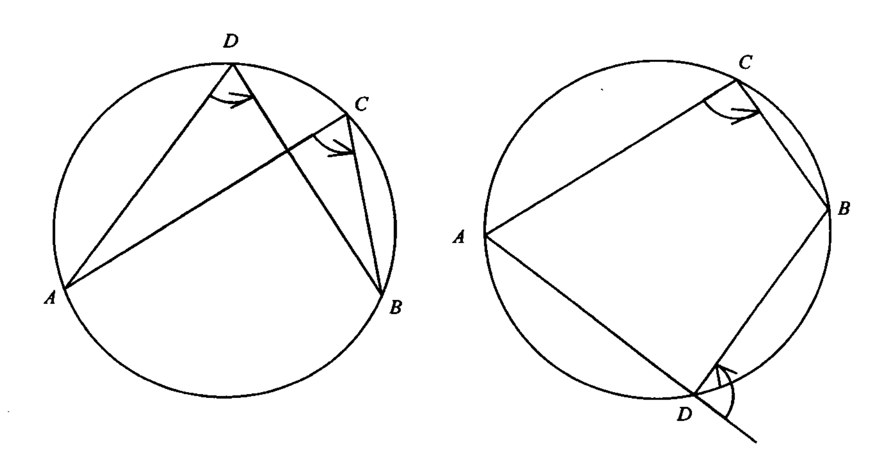


图 7.5　命题 7.2.12 的示意图

构造 2.8　定向角 $<(L_1, L_2)$ 的正切值是可以显式构造的.

构造 2.9　在普通平面上给定一个点 P 和一条直线 L, 过点 P 且具有给定 $<(L, L')$ 的正切值的直线 L' 是可以显式构造的.

定义 7.2.13　对于两条相交直线 L_1, L_2 的一个定向角 $<(L_1, L_2)$, 任意一条通过交点的直线 L 称为定向角的一条 平分线 当且仅当 $<(L_1, L_2) = 2* <(L_1, L)$.

定义 7.2.14　对于两条相交直线 L_1, L_2 的一个定向角 $<(L_1, L_2)$, 一条

通过交点的直线 L 称为定向角的一条 三等分线 当且仅当 $<(L_1,L_2)=3*<(L_1,L)$.

注释 7.2.15 对于相交的两条直线 L_1,L_2, 它们的定向角 $<(L_1,L_2)$ 有两条平分线和三条三等分线.

定义 7.2.16 设相交直线 L_1,L_2 的定向角 $<(L_1,L_2)$ 的任意一条三等分线为 L, L_1 相对于 L 的反射 L' 称为伴随于三等分线 L 的 第二条三等分线.

<u>涉及角度的 Hilbert 型几何定理</u>

借助于定向角的概念, 一些很难证明的定理可以转化为 Hilbert 型, 从而变得容易证明. 下面我们举几个例子加以说明.

例 7.2.17 (Steiner 定理) 在三角形 ABC 的三条边上同时向内或者向外作等边三角形 ABC',ACB',BCA', 则三条直线 AA',BB',CC' 共点.

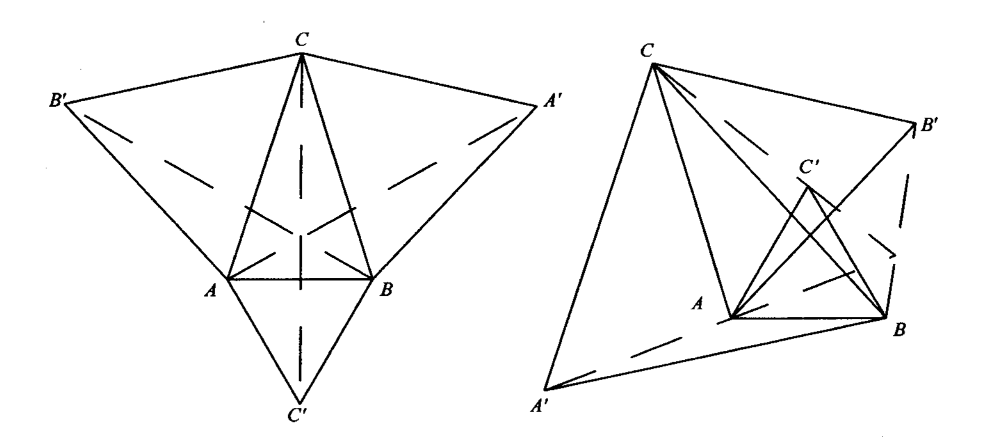


图 7.6 Steiner 定理

证明 取 $A=(x_1,0),B=(x_2,0),C=(0,x_3)$. 令 $\mathbf{Q}(m)$ 为 $\mathbf{Q}$ 的扩域, 其中 m 表示 $m^2=3$ (即 $m=\pm\ \tan\frac{\pi}{3}$). 设 AB', AC', BA', BC', CA', CB' 为通过 A,B,C 的直线, 满足

$$\left.\begin{aligned}\tan<(AC,AB')=\ \tan<(BA,BC')=\ \tan<(CB,CA')=m,\\ \tan<(AB,AC')=\ \tan<(BC,BA')=\ \tan<(CA,CB')=-m.\end{aligned}\right\}\tag{7.2.37}$$

由构造 2.8 与 2.1 知, 直线 $A'=(x_4,x_5)$, $B'=(x_6,x_7)$, $C'=(x_8,x_9)$ 的交点由

下面的方程给出：

$$\left.\begin{array}{ll} x_4 = \dfrac{m*x_3+x_2}{2}, & x_5 = \dfrac{m*x_2+x_3}{2}, \\ x_6 = \dfrac{-m*x_3+x_1}{2}, & x_7 = \dfrac{x_3-m*x_1}{2}, \\ x_8 = \dfrac{x_2+x_1}{2}, & x_9 = \dfrac{m*(-x_2+x_1)}{2}. \end{array}\right\} \tag{7.2.38}$$

结论 AA', BB', CC' 共点可以写成

$$CONC \equiv \begin{vmatrix} x_5 & x_1-x_4 & x_1*x_5 \\ x_7 & x_2-x_6 & x_2*x_7 \\ x_3-x_9 & x_8 & x_3*x_8 \end{vmatrix} = 0. \tag{7.2.39}$$

于是证明程序的指标集可以根据方案 (**) 如下执行:

$$CONC : [14\ x_9\ 1] \longrightarrow [18\ x_7\ 1] \longrightarrow [22\ x_5\ 1] \longrightarrow 0.$$ □

初等几何的一个著名定理是 Morley 定理，它涉及角的三等分线.

例 7.2.18 (Morley 定理) 已知三角形 ABC, 设 L_A, L_B, L_C 分别为定向角 $\angle(AB, AC), \angle(BC, BA), \angle(CA, CB)$ 的三等分线. 设 L'_A, L'_B, L'_C 分别为相应的另一个三等分线. 又设 D, E, F 为线段对 $(L_A, L'_B), (L_B, L'_C), (L_C, L'_A)$ 的交点. 如果

$$\angle(L_A, L'_A) + \angle(L_B, L'_B) + \angle(L_C, L'_C) = \pm\frac{\pi}{3}, \tag{7.2.40}$$

则三角形 DEF 是等边三角形.

证明 我们可以把坐标取为 $A=(x_1,0)$, $B=(x_2,0)$, $D=(0,x_3)$. 设 L_A, L'_A, AC 与 L'_B, L_B, BC 的斜率分别是 x_4, x_5, x_6 与 x_7, x_8, x_9. 参见图 7.7.

由构造 2.1 与 2.4, 我们有

$$\left.\begin{array}{lll} x_4 = -\dfrac{x_3}{x_1}, & x_5 = \dfrac{2*x_4}{1-x_4^2}, & x_6 = \dfrac{3*x_4-x_4^3}{1-3*x_4^2}, \\ x_7 = -\dfrac{x_3}{x_2}, & x_8 = \dfrac{2*x_7}{1-x_7^2}, & x_9 = \dfrac{3*x_7-x_7^3}{1-3*x_7^2}. \end{array}\right\} \tag{7.2.41}$$

直线 AC, BC 的交点为 $C=(x_{10}, x_{11})$, 满足

$$x_{10} = \frac{x_9*x_2-x_6*x_1}{x_9-x_6}, \quad x_{11} = x_6*(x_{10}-x_1). \tag{7.2.42}$$

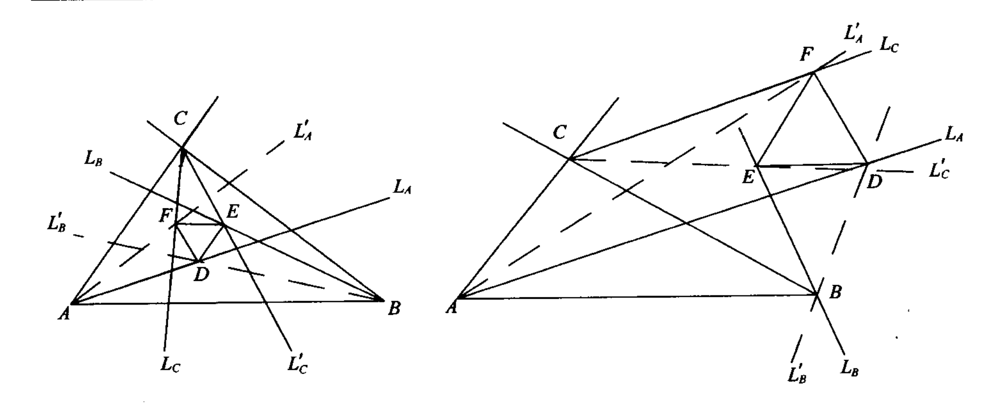


图 7.7 Morley 定理

令 $\tan(\pm\frac{\pi}{3}) = a$, 于是 $a^2 = 3$. 现在令 $\tan < (L_C, L'_C) = x_{12}$ 以及 L_C, L'_C 的斜率分别为 x_{13}, x_{14}. 于是我们有

$$\left.\begin{aligned} x_{12} &= \frac{-x_4 + x_7 + a + x_4 * x_7 * a}{1 + x_4 * x_7 + x_4 * a - x_7 * a}, \\ x_{13} &= \frac{x_{12} + x_6}{1 - x_{12} * x_6}, \quad x_{14} = \frac{x_{12} + x_{13}}{1 - x_{12} * x_{13}}. \end{aligned}\right\} \tag{7.2.43}$$

最后, 交点 $E = (x_{15}, x_{16}), F = (x_{17}, x_{18})$ 由

$$\begin{aligned} x_{15} &= \frac{x_{14} * x_{10} - x_8 * x_2 - x_{11}}{x_{14} - x_8}, \quad x_{16} = x_8 * (x_{15} - x_2), \\ x_{17} &= \frac{x_{13} * x_{10} - x_5 * x_1 - x_{11}}{x_{13} - x_5}, \quad x_{18} = x_5 * (x_{17} - x_1) \end{aligned} \tag{7.2.44}$$

给出. 方程 (7.2.41)~(7.2.44) 形成了假设系统. 结论是 $|DE|^2 = |DF|^2 = |EF|^2$. 由对称性知, 只需证明 $|DE|^2 = |DF|^2$, 或

$$CONC \equiv x_{17}^2 + (x_{18} - x_3)^2 - x_{15}^2 - (x_{16} - x_3)^2 = 0.$$

如果我们首先把每一个 $x_i (i = 8, \cdots, 19)$ 约化为 $\frac{P'_i}{Q'_i}$ 的形式, 其中 P'_i, Q'_i 是 x_1, x_2, x_3 的如同 (7.2.21) 的多项式, 则证明过程的指标集可以根据方案 (**) 如下执行:

$$CONC\colon [8\ x_{18}\ 2] \longrightarrow [125\ x_{16}\ 2] \longrightarrow 0, \qquad \square$$

注释 7.2.19 如果我们直接从 (7.2.20) 执行方案 (**), 则出现在证明过程中的多项式集将迅速地增加到上千项, 并导致证明失败.

注释 7.2.20　每一个定向角 $<(AB,AC)$, $<(BC,BA)$, $<(CA,CB)$ 有三条三等分线，所以一共可以组成 27 个三角形 DEF. 但是，在 (7.2.43) 的限制下，只有 18 个被证明是等边的. 事实上，其余的 9 个三角形一般不是等边的.

6- 极点定理

下面是另一个涉及角的几何定理证明的例子，该例子是考察一个平面 E 在一个固定的平面 E_0 上的移动. E 从一个位置到另一个位置的运动是一个平移或者是一个旋转.

定义 7.2.21　对于一个在一个固定的平面上从一个位置到另一个位置移动的活动平面的旋转中心称为旋转的 *极点*.

记号 7.2.22　一个在固定的平面上移动的活动平面从一个位置 E_i 到另一个位置 E_j 旋转的极点和旋转角分别记为是 P_{ij} 和 θ_{ij}. 显然 $P_{ij}=P_{ji}$ 并且 θ_{ij} 在相差 $2*\pi$ 的倍数的意义下是唯一确定的，其中 $\theta_{ij}=-\theta_{ji}\ (\mathrm{mod}\ 2*\pi)$.

下面的命题是一个著名的命题，并且是机械装置研究运动学分析中的基本命题.

命题 7.2.23　一个活动平面在一个固定平面上运动的三个位置为 E_i,E_j,E_k. 假设从一个位置到另一个位置的运动都是旋转，则有

$$<(P_{ij}P_{ik},P_{ij}P_{jk})=\frac{\theta_{ij}}{2},\tag{7.2.45}$$

该等式是在 $\mathrm{mod}\ \pi$ 同余的意义下成立.

例 7.2.24 (6- 极点定理)　设一个活动平面在固定平面上的运动有四个位置不同的点 E_i, $i=1,2,3,4$, 其中从一个位置 E_i 到另一个位置 E_j 的旋转的极点为 P_{ij}, 旋转角为 θ_{ij}, 则三对极点 $(P_{12},P_{34}),(P_{13},P_{24}),(P_{14},P_{23})$ 的中点 $M_{12,34},M_{13,24}$, $M_{14,23}$ 共线.

证明　点 $P_{12},P_{13},P_{23},P_{14}$ 可以任意选取，所以我们可以把坐标取为

$$P_{12}=(0,0),\quad P_{13}=(x_1,0),\quad P_{23}=(x_2,x_3),\quad P_{14}=(x_4,x_5),$$

点 P_{24} 不是可以随意选取的，由命题 7.2.23 可知，它被下面的条件约束：

$$<(P_{12}P_{13},P_{12}P_{23})=<(P_{12}P_{14},P_{12}P_{24})\ \left(=\frac{\theta_{12}}{2}\right).$$

于是直线 $P_{12}P_{24}$ 有下面的形式：

$$(x_4*x_2-x_5*x_3)*Y_1=(x_4*x_3+x_5*x_2)*Y_2.$$

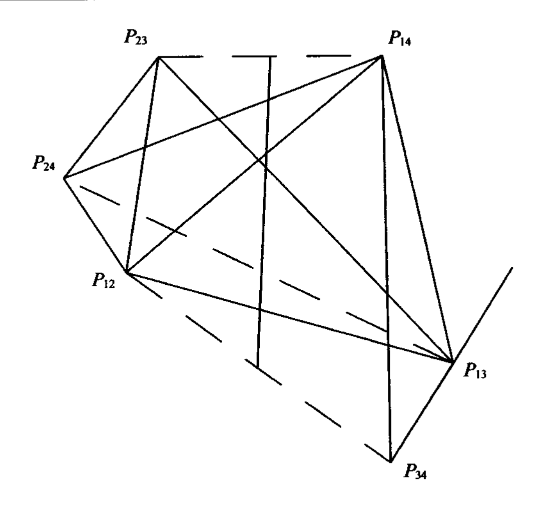


图 7.8 6- 极点定理

因此，我们可以在这条直线上取任意一点 $P_{24}=(x_6,x_7)$，使得 x_0 是任意常数并且

$$x_6=(x_4*x_2-x_5*x_3)*x_0, \quad x_7=(x_4*x_3+x_5*x_2)*x_0. \tag{7.2.46}$$

根据命题 7.2.23, 直线 $P_{13}P_{34}$ 与 $P_{14}P_{34}$ 之间有下面的限制关系：

$$<(P_{13}P_{14},P_{13}P_{34})=<(P_{13}P_{12},P_{13}P_{23})\ (=\frac{\theta_{13}}{2}),$$

其正切值为 $x_3:(x_2-x_1)$. 由构造 2.9 知直线 $P_{13}P_{34}$ 的斜率为 $x_8:x_9$, 其中

$$\left.\begin{aligned} x_8&=-(x_4-x_1)*x_3-x_5*(x_2-x_1),\\ x_9&=-(x_4-x_1)*(x_2-x_1)+x_5*x_3. \end{aligned}\right\} \tag{7.2.47}$$

相似地，我们有

$$<(P_{14}P_{13},P_{14}P_{34})=<(P_{14}P_{12},P_{14}P_{24})\ \left(=\frac{\theta_{13}}{2}\right),$$

其正切值为 $x_{10}:x_{11}$, 其中

$$\left.\begin{aligned} x_{10}&=-\ x_5*(x_6-x_4)+x_4*(x_7-x_5),\\ x_{11}&=x_4*(x_6-x_4)+x_5*(x_7-x_5). \end{aligned}\right\} \tag{7.2.48}$$

从而直线 $P_{14}P_{34}$ 的斜率为 $x_{12}:x_{13}$, 其中

$$\left.\begin{aligned} x_{12} &= -(x_4 - x_1) * x_{10} - x_5 * x_{11}, \\ x_{13} &= -(x_4 - x_1) * x_{11} + x_5 * x_{10}. \end{aligned}\right\} \tag{7.2.49}$$

由构造 2.1, 点 $P_{34}=(x_{14},x_{15})$ 由下面的公式给出:

$$\left.\begin{aligned} x_{14} &= \frac{x_{13} * x_9 * x_5 + x_{13} * x_8 * x_1 - x_{12} * x_9 * x_4}{x_{13} * x_8 - x_{12} * x_9}, \\ x_{15} &= \frac{x_8 * (x_{13} * x_5 - x_{12} * x_4 + x_{12} * x_1)}{x_{13} * x_8 - x_{12} * x_9}. \end{aligned}\right\} \tag{7.2.50}$$

于是, 中点为

$$\begin{gathered} M_{12,34} = \left(\frac{x_{14}}{2}, \frac{x_{15}}{2}\right), \quad M_{13,24} = \left(\frac{x_6 + x_1}{2}\ \frac{x_7}{2}\right), \\ M_{14,23} = \left(\frac{x_4 + x_2}{2}, \frac{x_5 + x_3}{2}\right). \end{gathered} \tag{7.2.51}$$

结论可以写成如下的形式:

$$CONC \equiv \begin{vmatrix} x_{14} & x_{15} & 1 \\ x_6 + x_1 & x_7 & 1 \\ x_4 + x_2 & x_5 + x_3 & 1 \end{vmatrix} = 0.$$

证明过程的指标集可以根据方案 (**) 如下执行:

$$\begin{aligned} CONC : [13\ x_{15}\ 1] &\longrightarrow [24\ x_{13}\ 1] \longrightarrow [46\ x_{11}\ 1] \longrightarrow [54\ x_9\ 1] \\ &\longrightarrow [83\ x_7\ 2] \longrightarrow 0. \end{aligned}$$

□

一个三次曲线的定理

显式构造及其相应的几何定理证明方法并不是仅仅局限于初等几何和它的类似的几何. 例如, 我们有下面的

构造 2.10 给定射影平面中的一条三次曲线及其上面两点. 这两点的连线与三次曲线的另一交点是可以显式构造的.

例 7.2.25 (三次合冲定理) 设 $P_i(i=1,\cdots,8)$ 为射影平面上三次曲线 C 上 8 个点, 满足这些点的三元组 $P_1,P_2,P_5;P_3,P_4,P_6;P_1,P_3,P_7;\ P_2,P_4,P_8$ 都是共线的, 则直线 P_5P_6,P_7P_8 的交点 P_9 也在三次曲线上.

证明 取齐次坐标 $(Y_1:Y_2:Y_3)$ 满足

$$P_1=(1:0:0),\ P_2=(0:1:0),\ P_3=(0:0:1),\ P_4=(1:1:1).$$

于是，三次曲线 C 有如下形式的方程：

$$\left.\begin{aligned}&x_1*Y_1*Y_2*(Y_1-Y_3)+x_2*Y_1*Y_3*(Y_1-Y_2)\\&+x_3*Y_1*Y_2*(Y_2-Y_3)+x_4*Y_2*Y_3*(Y_2-Y_1)\\&+x_5*Y_3*Y_1*(Y_3-Y_2)+x_6*Y_2*Y_3*(Y_3-Y_1)=0.\end{aligned}\right\}\tag{7.2.52}$$

由构造 2.10 知道，点 $P_j(j=5,6,7,8)$ 由

$$P_5=(x_3:-x_1:0),\quad P_6=(x_5+x_6:x_5+x_6:x_1+x_3),$$
$$P_7=(x_5:0:-x_2),\quad P_8=(x_3+x_4:x_2+x_5:x_3+x_4)$$

给出. 类似于构造 2.1, 点 $P_9=(x_7:x_8:x_9)$ 由

$$\left.\begin{aligned}x_7&=x_6*x_4+x_6*x_3+x_5*x_4,\\x_8&=x_6*x_2+x_5*x_2+x_5*x_1,\\x_9&=x_4*x_1+x_3*x_2+x_3*x_1\end{aligned}\right\}\tag{7.2.53}$$

给出. 要证明的结论是，点 P_9 在三次曲线上，即

$$\begin{aligned}CONC\equiv\ &x_1*x_7*x_8*(x_7-x_9)+x_2*x_7*x_9*(x_7-x_8)\\&+x_3*x_7*x_8*(x_8-x_9)+x_4*x_8*x_9*(x_8-x_7)\\&+x_5*x_9*x_7*(x_9-x_8)+x_6*x_8*x_9*(x_9-x_7)=0.\end{aligned}$$

根据方案 (**), 定理的证明可以按照下面的次序进行：

$$CONC:[12\ x_9\ 2]\longrightarrow[36\ x_8\ 2]\longrightarrow[60\ x_7\ 2]\longrightarrow 0.$$ □

§7.3 只涉及等式的几何定理机器证明

在前面一节，我们看到，通过细致的思考，许多几何定理可以出乎意料的整理为 Hilbert 型的定理. 但也有很多定理要整理为 Hilbert 型的定理实际上是不可能的. 为了避免最终可能的这种人为的处理，我们继续沿着更自然的路线，我们只考虑范围 **E** 中的定理，这些定理只与等式有关，并不涉及不等式，则我们可以应用机械化定理证明的三个原理. 首先，我们考虑最简单的机械化证明原理 I.

基于整序原理的机械化证明原理 I 的例子

为了方便读者，下面再介绍一次机械化证明原理 I.

机械化证明原理 I 在范围 **E** 中，对于给定的定理 $T=\{HYP,CONC\}$，令 CS 是多项式集合 HYP 的特征列，那么

$$R\equiv\text{Remdr}(CONC/CS)=0\tag{7.3.54}$$

是对于定理 T 在 非退化条件 $IP=0$ 下 一般正确 的充分条件，这里 IP 是特征集 CS 的初式积. 更进一步，$R=0$ 也是在 CS 是不可约升列时，上式成立的必要条件.

例 7.3.1 (8-3 元组定理) 从 8 个互不相同的点 $A_i(i=1,\cdots,8,A_{i+8}=A_i)$ 中可以取出 8 个组 $T_i=A_iA_{i+1}A_{i+3}$，$i=1,\cdots,8$. 如果这些组是共线的，那么 一般说来 组 $A_1A_2A_3$ 也是共线的，并且事实上 一般说来 这 8 个点是共线的.

证明 我们称包含 8 个互不相同的点 $A_i=(x_i,y_i)(i=1,\cdots,8,A_{i+8}=A_i)$，并且 $T_i=A_iA_{i+1}A_{i+3}(i=1,\cdots,8)$ 是共线的图形为 8-3元组 图形. 如果 8 个点 A_i 不共线，称这个图形是 非平凡的. 对于给定的 8-3 元图形，取坐标为

$$A_1=(0,0),\quad A_2=(x_2,0),\quad A_i=(x_i,y_i),\quad i=3,\cdots,8, \tag{7.3.55}$$

那么 $T_1=A_1A_2A_4$ 共线推出 $y_4=0$，$T_i(i=2,\cdots,8)$ 共线给出假设多项式集 $HYP=\{P_1,\cdots,P_7\}$，其中 P_i 如下：

$$\left.\begin{aligned}
&P_1=y_5*(x_3-x_2)-y_3*(x_5-x_2),\\
&P_2=y_6*(x_4-x_3)+y_3*(x_6-x_4),\\
&P_3=y_7*(x_5-x_4)-y_5*(x_7-x_4),\\
&P_4=y_8*(x_6-x_5)-y_6*(x_8-x_5)+y_5*(x_8-x_6),\\
&P_5=y_7*x_6-y_6*x_7,\\
&P_6=y_8*(x_7-x_2)-y_7*(x_8-x_2),\\
&P_7=y_8*x_3-y_3*x_8.
\end{aligned}\right\} \tag{7.3.56}$$

注意到 $A_1A_2A_3$ 共线将推出图形是平凡的. 如果假定 $A_1A_2A_3$ 共线将有 $y_3=0$，这样

$$\begin{aligned}
y_3=0\quad &\Longrightarrow_{(A_3\neq A_2)}\ x_3\neq x_2\ \Longrightarrow_{(P_1=0)}\ y_5=0\\
&\Longrightarrow_{(A_5\neq A_4)}\ x_5\neq x_4\ \Longrightarrow_{(P_3=0)}\ y_7=0\\
&\Longrightarrow_{(A_4\neq A_3)}\ x_4\neq x_3\ \Longrightarrow_{(P_2=0)}\ y_6=0\\
&\Longrightarrow_{(A_6\neq A_5)}\ x_6\neq x_5\ \Longrightarrow_{(P_4=0)}\ y_8=0.
\end{aligned}$$

从而 8 个点 A_i 共线，这样，图形是平凡的.

取序为

$$x_2\prec x_3\prec x_4\prec x_5\prec x_6\prec x_7\prec x_8\prec y_3\prec y_5\prec y_6\prec y_7\prec y_8. \tag{7.3.57}$$

HYP 的特征集是 $CS=\{C_1,\cdots,C_5\}$，

$$C_1=y_3*I_1,\quad C_i=P_{i-1},\quad i=2,\cdots,5,$$

这里 I_1 的指标集是 [12 x_7 1]. CS 的初式积是

$$IP = I_1 * (x_3 - x_2) * (x_4 - x_3) * (x_5 - x_4) * (x_6 - x_5).$$

这样，定理在非退化条件

$$I_1 \neq 0, \quad x_3 \neq x_2, \quad x_4 \neq x_3, \quad x_5 \neq x_4,\ x_6 \neq x_5$$

下 一般 成立. 如果把 I_1 添加到 HYP, 新的多项式集 HYP' 的特征集 $CS' = \{I_1, y_3 * I_2, C_2, \cdots, C_5\}$, 其中 $C_i (i = 2, \cdots, 5)$ 与以上相同并且

$$I_2 = (x_4 - x_2) * I_2',$$

这里 I_2' 的指标集是 [24 x_8 1]. 因此，如果有 $I_1 = 0$ 但 $x_4 \neq x_2, I_2' \neq 0$, 那么定理 一般 成立. 如果把 I_1, I_2' 都添加到 HYP, 由以上方法得到新的多项式集的特征集 $CS'' = \{I_1, I_2', y_3 * I_3, C_2, \cdots, C_5\}$, 其中

$$I_3 = (x_6 - x_5) * (x_5 - x_4) * (x_4 - x_3) * (x_3 - x_2) * I_3'',$$

I_3'' 的指标集是 [20 x_6 2]. 由此推出，在非退化条件 $x_i \neq 0, x_i \neq x_j$ 其中 $i, j = 2, \cdots, 8, i \neq j$ 并且 I_1, I_2', I_3'' 之一不为零时，定理成立. □

注释 7.3.2 从例 7.3.1 可以看到非退化条件是如此复杂，没有任何明显的几何意义且难以预见. 当然这里的方法可以自动找出非退化条件.

注释 7.3.3 从证明中可见，如果 $x_i (i = 1, \cdots, 8)$ 互异且 I_1, I_2', I_3'' 都为零, 那么定理不再成立. 实际上, 在某些扩展的仿射空间存在 ∞^8 图形 (例如, 复空间), 使得所有的 A_i 互异并且所有的 $A_i A_{i+1} A_{i+3}$ 共线但 $A_1 A_2 A_3$ 不共线. 这个情形在 实 仿射空间上将完全不同 (见例 7.4.8).

例 7.3.4 (Desargues 定理) $ABC, A'B'C'$ 是两个三角形，对应边两两平行. AA', BB' 相交于点 O, 那么, CC' 也过点 O.

证明 这是在例 2.1.5 和例 3.6.32 中考虑的定理的一部分. 我们可以容易地用显示构造的形式表示这个定理，然后像上节一样证明. 可是，为了说明我们更一般的方法，这里采用另一种方法. 为了证明这个定理，我们像例 3.6.32 一样取坐标，即

$$A = (x_1, 0), \quad B = (0, x_3), \quad C = (x_4, x_5),$$
$$A' = (x_2, 0), \quad B' = (0, x_6), \quad C' = (x_7, x_8),$$

则假设多项式集 $HYP = \{H_1, H_2, H_3\}$ 像例 3.6.32 一样，我们重写为

$$\left.\begin{aligned} H_1 &= x_1 * x_6 - x_2 * x_3, \\ H_2 &= x_4 * (x_8 - x_6) - x_7 * (x_5 - x_3), \\ H_3 &= (x_4 - x_1) * x_8 - x_5 * (x_7 - x_2). \end{aligned}\right\} \tag{7.3.58}$$

结论多项式为

$$CONC = x_4 * x_8 - x_5 * x_7. \tag{7.3.59}$$

多项式集 $HYP = \{H_1, H_2, H_3\}$ 不是升列形式. 容易得到其特征列为 $CS = \{C_1, C_2, C_3\}$, 其中

$$\left.\begin{aligned} &C_1 = H_1, \\ &C_2 = x_7 * (x_1 * x_3 - x_1 * x_5 - x_3 * x_4) + x_4^2 * x_6 \\ &\qquad + x_2 * x_4 * x_5 - x_2 * x_3 * x_4, \\ &C_3 = H_3. \end{aligned}\right\} \tag{7.3.60}$$

于是, 可以验证 (7.3.54) 成立. 因此定理在非退化条件

$$I_1 \equiv x_1 \neq 0, \quad I_2 \equiv x_1 * x_3 - x_1 * x_5 - x_3 * x_4 \neq 0, \quad I_3 \equiv x_4 - x_1 \neq 0$$

下一般成立, 其中 I_1, I_2, I_3 分别为 C_1, C_2, C_3 的初式.

注释 7.3.5 $I_2 \neq 0$ 这个条件意味着三角形 ABC 不会退化成一条直线. 在图 3.2 或图 3.6 中可见, 这个条件是不可缺少的. 实际上, 把 I_2 添加到 HYP, 再求出特征集, 此时结论多项式的余式不再为零, 所以当三角形 ABC 退化成直线时, 定理不再成立.

注释 7.3.6 非退化条件 $I_3 \neq 0$ 意味着 AC 不与 Y 轴平行. 为了看到这个条件对于定理的正确性是否真的必要, 我们可以把新的假设多项式 I_3 加入 HYP, 决定其特征集和结论多项式关于这个特征列的余式, 容易发现, 此余式为 0, 所以定理在非退化条件下仍然成立, 见图 3.5. 对任何非退化条件, 如果值得做, 则我们将继续做同样的过程. 这种方法可以运用到 $\mathbf{E}$ 类中的任何定理.

注释 7.3.7 退化条件 $I_1 = x_1 = 0$ 意味着 A_1 与 O 重合. 为了要看到定理是否在某种 退化 意义下仍然成立, 我们可以把多项式 x_1 加入 HYP, 形成一个新的假设集, 然后继续用前面的方法做, 看在这种情形下会发生什么结论. 这个过程很复杂和冗长, 没有什么几何意义, 所以这里就不做了.

注释 7.3.8 假定一个在范围 $\mathbf{E}$ 的定理 $T = \{HYP, CONC\}$ 的成立是指

$$HYP = 0 \longrightarrow CONC = 0. \tag{7.3.61}$$

根据 Hilbert 零点定理, 这等价于对于某个正整数 k,

$$CONC \in \text{Ideal}(HYP). \tag{7.3.62}$$

对于由 (7.3.58) 和 (7.3.59) 给出的 $HYP, CONC$ 所描述的 Desargues 定理，我们容易看到 (7.3.62) 不成立．例如，点 $(x_1, \cdots, x_8) = (2,4,1,1,2,4,3,1)$ 满足方程 $\mathrm{Ideal}(HYP) = 0$ 或 $HYP = 0$ 但不满足 $CONC = 0$(参见例 3.6.32 和图 3.6)．这表明对于几何定理证明，仅用理想论处理是不够的．其根本原因在于通常关于不等方程形式的非退化条件很难用理想论处理．这就是我们在当前的研究中不用理想理论，而用零点集理论处理的一个原因．

基于机械化定理证明原理 II 的几何定理证明的示例

虽然机械化定理证明原理 I 对于几何定理证明容易运用，但是非常不完备．为了得到更多的信息，就要用到基于零点分解定理的机械化定理证明原理 II.

机械化定理证明原理 II. 在域 **E** 上, 对于给定的定理 $T = \{HYP, CONC\}$ 令 AS_i 为从假设集 HYP 得到的升列:

$$\mathrm{Zero}(HYP) = \bigcup_i \mathrm{Zero}(AS_i/IP_i), \tag{7.3.63}$$

其中 IP_i 为 AS_i 的初式积．那么，定理 T 在 $\mathrm{Zero}(AS_i/IP_i)$ 上成立，也就是

$$\mathrm{Zero}(AS_i/IP_i) \subset \mathrm{Zero}(CONC) \tag{7.3.64}$$

如果

$$\mathrm{Remdr}(CONC/AS_i) = 0. \tag{7.3.65}$$

例 7.3.9 (修正的例 7.3.4) 我们再考虑例 7.3.4 或 3.6.32 中的 Desargues 定理．像例 3.6.32 一样，我们考虑把 x_1, x_2, x_3 作为非零独立常数参数．那么，我们有 3.6.139, 也就是

$$\mathrm{Zero}(HYP) = \bigcup_{i=1}^{5} \mathrm{Zero}(AS_i/IP_i), \tag{7.3.66}$$

AS_i 是 (3.6.140) 的升列， IP_i 是对应的初式积．容易发现

$$\left.\begin{array}{ll} \mathrm{Remdr}(CONC/AS_i) = 0, & i = 1,5, \\ \mathrm{Remdr}(CONC/AS_i) \neq 0, & i = 2,3,4. \end{array}\right\} \tag{7.3.67}$$

由机械化定理证明原理 II 可知，定理在第一和最后部分成立，而其余 3 部分并不显然，这与几何情形一致．见图 3.1~3.5.

注释 7.3.10 在 (7.3.63) 和 (7.3.66) 中 Zero(HYP) 的分解通常不是唯一的. 即使我们通过加入非零条件来除掉无意义的和不合意的分支, 分解中的分支仍然可能很多. 尽管如此, 机械化定理证明原理 II 为我们提供的关于一个定理的真实性的信息远比原理 I 完备.

基于机械化定理证明原理 III 的几何定理证明

机械化定理证明原理 III 对于范围 $\mathbf{E}$ 上给定的定理 $T = \{HYP, CONC\}$, 令 IRR_k 为假设多项式集 HYP 决定的不可约升列集, 使得

$$\text{Zero}(HYP) = \bigcup_k \text{Var}[IRR_k], \tag{7.3.68}$$

那么定理 T 在不可约分支 Var[IRR_k] 上成立的充要条件是

$$\text{Remdr}(CONC/IRR_k) = 0. \tag{7.3.69}$$

例 7.3.11 (例 7.3.4 和修改的例 7.3.9 的进一步探讨) 这里再考虑 Desargues 定理. 由于在 (7.3.66) 中的升列 AS_i 都是不可约的, 将 AS_i 重命名为 IRR_i, 那么 (7.3.63) 中 Zero(HYP) 的分解具有 (3.6.143) 的形式 (x_1, x_2, x_3 作为非零常数, HYP 由 (7.3.58) 给出), 即

$$\text{Zero}(HYP) = \text{Var}[IRR_1] + \text{Var}[IRR_2]. \tag{7.3.70}$$

由此得出

$$\text{Remdr}(CONC/IRR_1) = 0,$$

而

$$\text{Remdr}(CONC/IRR_2) \neq 0.$$

由机械化定理证明原理 III 可知, Desargues 定理在不可约分支 Var[IRR_1] 上成立, 但在分支 Var[IRR_2] 上不成立. 其几何原因是显然的. 参见注释 7.3.13.

注释 7.3.12 在 (7.3.70) 中的分解与 (7.3.63) 中的不同, 不含多余分支的分解在不记次序的前提下是唯一的. 事实上, 与机械化定理证明原理 I, II 相比, 机械化定理证明原理 III 给出了关于几何定理真实性的更多的信息. 可是, 为了得到 (7.3.68), 需要代数函数域上多项式的分解, 而这是一个不容易的工作. 就几何定理证明而言, 尽管原理 I 是不完备的, 但好像还是应该先使用它, 因为定理 *一般* 成立已经足够达到我们的目的. 对于这一点, 参见注释 7.3.6.

例 7.3.13 (内心或外心定理) 三角形的角平分线三三交于四点.

证明 设三角形 ABC 顶点为 $A=(x_1,0)$, $B=(x_2,0)$, $C=(0,x_3)$, 角 A,B,C 的平分线为 AD,BD,CE. 设 $D=(x_4,x_5)$, CE 的斜率是 $x_7:x_6$. 那么假设多项式集是 $HYP=\{H_1,\cdots,H_5\}$, 其中 H_i 为

$$\left.\begin{aligned}H_1&=x_5^2*x_3-2*x_5*x_1*(x_4-x_1)-x_3*(x_4-x_1)^2,\\H_2&=x_5^2*x_3-2*x_5*x_2*(x_4-x_2)-x_3*(x_4-x_2)^2,\\H_3&=x_7^2*x_3*(x_2+x_1)+2*x_7*x_6*(x_3^2-x_1*x_2)\\&\quad-x_6^2*x_3*(x_2+x_1),\end{aligned}\right\}\tag{7.3.71}$$

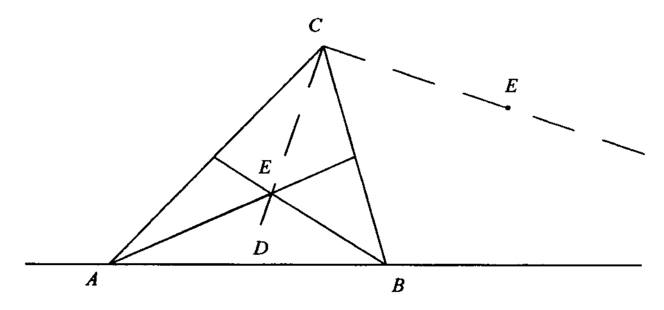


图 7.9 内心或外心定理

对应于角平分线 AD,BD,CF 或交于一点或者 CF 在点 D 上, 结论多项式为

$$CONC=x_4*x_7-x_6*(x_5-x_3).\tag{7.3.72}$$

HS 的特征集为 $CS=\{C_1,C_2,C_3\}$, 其中:

$$\left.\begin{aligned}C_1&=-4*x_4^4+8*x_4^3*(x_1+x_2)\\&\quad-4*x_4^2*(x_1^2+3*x_1*x_2+x_2^2-x_3^2)\\&\quad-4*x_4*(x_1+x_2)*(x_3^2-x_1*x_2)+x_3^2*(x_1+x_2)^2,\\C_2&=2*x_5*(x_4-x_1-x_2)-x_3*(2*x_4-x_1-x_2),\\C_3&=x_7^2*x_3*(x_1+x_2)+2*x_7*x_6*(x_3^2-x_1*x_2)\\&\quad-x_6^2*x_3*(x_1+x_2).\end{aligned}\right\}\tag{7.3.73}$$

我们看到 (7.3.54) 不成立, 因此尽管定理在几何上显然但定理不真 (参见图 7.9). 实际上, 特征集 CS 不是不可约的. 如果应用机械化定理证明原理 III, 将得到 (把 x_1,x_2,x_3 考虑为独立参数)

$$\text{Zero}(HYP)=\text{Var}[IRR_1]+\text{Var}[IRR_2].\tag{7.3.74}$$

在 (7.3.74) 中，不可约升列为 $IRR_i = \{C_1, C_2, C_{i3}\}$, $i = 1, 2$, 其中

$$\left.\begin{aligned} C_{13} &= 2 * x_7 * x_4 * (x_4 - x_1 - x_2) - x_6 * x_3 * (x_1 + x_2), \\ C_{23} &= x_7 * x_3 * (x_1 + x_2) + 2 * x_6 * x_4 * (x_4 - x_1 - x_2). \end{aligned}\right\} \quad (7.3.75)$$

(7.3.69) 在第一个分支上是成立的，但在 (7.3.74) 的第二个分支上不成立. 这对应于如下的一个几何事实：$\angle C$ 的两条分角线之一过点 D, 而另一条却不过点 D. 角平分线共点的三元组数是 4, 对应于 4 个可能由 $C_1 = 0$ 和 $C_2 = 0$ 给出的内心或外心 D.

在几何中，对应于非显式构造有许多歧义，以致在上面的应用机械化定理证明原理中可能会引起很多问题. 为了说明这种歧义性，不妨看看以下几个情形.

歧义性 1. 无法区分直线与圆相交的两个不同的点.

歧义性 2. 无法区分通过圆外一点与该圆相切的两条切线.

歧义性 3. 无法区分两条相交直线的交角的两条角平分线.

歧义性 4. 对于互异的两个圆，无法区分它们的四条公切线.

示例：割线定理

作为一个例子，来看看歧义性会有什么样的问题，我们考虑下面的简单的有争论的割线定理.

例 7.3.14 (割线定理) 从点 S, 作两条割线分别交圆于点 A_1, A_1' 和 A_2, A_2', 那么，割线长乘积相等，即

$$|SA_1| * |SA_1'| = |SA_2| * |SA_2'|. \quad (7.3.76)$$

见图 7.10.

现在下面用 错误 的方式应用机械化定理证明原理试图来证明这个定理. 令点 S 为 (x_0, y_0), 同时圆 C 和直线 L_1, L_2 分别过点 S,

$$\left.\begin{aligned} C\text{:}\ X^2 + Y^2 &= 1, \\ L_i\text{:}\ a_i * (X - x_i) &= b_i * (Y - b_i),\ i = 1, 2. \end{aligned}\right\} \quad (7.3.77)$$

在 (7.3.77) 中，X, Y 是活动坐标，a_i, b_i 是未定常数. 点 A_i, A_i' 由以下给出：

$$A_i = (x_i, y_i), \quad A_i' = (x_i', y_i'), \quad i = 1, 2, \quad (7.3.77')$$

距离 SA_1, SA_1', SA_2, SA_2' 分别为 z_1, z_1', z_2, z_2'. 这样有假设多项式集 $HYP =$

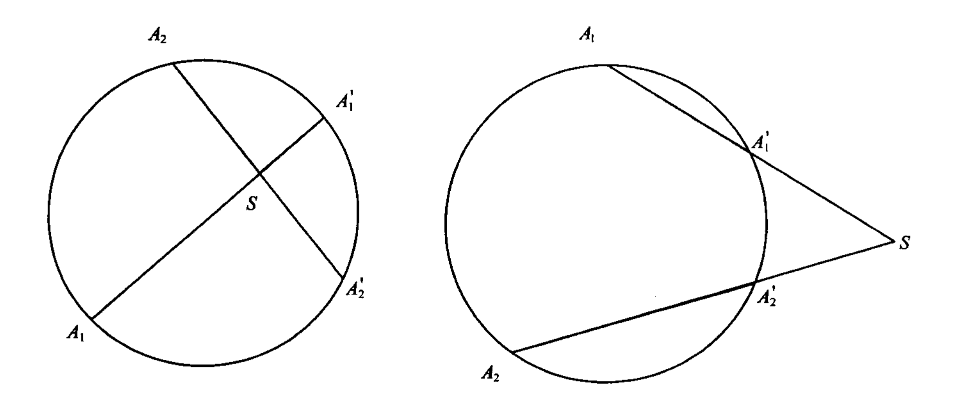


图 7.10 割线定理

$\{H_1, \cdots, H_{12}\}$, 其中 H_i 如下给出:

$$\left.\begin{aligned}
H_1 &= (a_1^2+b_1^2)*x_1^2+2*a_1*x_1*(b_1*y_0-a_1*x_0)\\
&\quad +(b_1*y_0-a_1*x_0)^2-b_1^2,\\
H_2 &= b_1*(y_1-y_0)-a_1*(x_1-x_0),\\
H_3 &= (a_1^2+b_1^2)*x_1'^2+2*a_1*x_1'*(b_1*y_0-a_1*x_0)\\
&\quad +(b_1*y_0-a_1*x_0)^2-b_1^2,\\
H_4 &= b_1*(y_1'-y_0)-a_1*(x_1'-x_0),\\
H_5 &= (a_1^2+b_1^2)*x_2^2+2*a_1*x_2*(b_1*y_0-a_1*x_0)\\
&\quad +(b_1*y_0-a_1*x_0)^2-b_1^2,\\
H_6 &= b_1*(y_2-y_0)-a_1*(x_2-x_0),\\
H_7 &= (a_1^2+b_1^2)*x_2'^2+2*a_1*x_2'*(b_1*y_0-a_1*x_0)\\
&\quad +(b_1*y_0-a_1*x_0)^2-b_1^2,\\
H_8 &= b_1*(y_2'-y_0)-a_1*(x_2'-x_0),\\
H_9 &= z_1^2-(x_1-x_0)^2-(y_1-y_0)^2,\\
H_{10} &= z_1'^2-(x_1'-x_0)^2-(y_1'-y_0)^2,\\
H_{11} &= z_2^2-(x_2-x_0)^2-(y_2-y_0)^2,\\
H_{12} &= z_2'^2-(x_2'-x_0)^2-(y_2'-y_0)^2,
\end{aligned}\right\} \tag{7.3.78}$$

结论多项式为

$$CONC = z_2^2*z_2'^2-z_1^2*z_1'^2. \tag{7.3.79}$$

我们取变量序为

$$x_0 \prec y_0 \prec x_1 \prec y_1 \prec x_1' \prec y_1' \prec x_2 \prec y_2 \prec x_2' \prec y_2' \prec z_1 \prec z_1' \prec z_2 \prec z_2'. \tag{7.3.80}$$

假设多项式集 HYP 已经是升列形式. 容易证明

$$\text{Remdr}(CONC/HYP) \neq 0. \tag{7.3.81}$$

从机械化定理证明原理, 由以上方法没有得出结论肯定割线定理是否成立. 可是, 我们也不可能草率地得出割线定理不成立的结论. 事实上, 这是一个著名的正确的定理. 这个好像矛盾的结论是由于对机械化定理证明原理 I 的误解. 事实上, 原理只是说明, 结论多项式的余式为零仅仅是定理 一般 成立的充分条件, 而不是必要条件. 只有当讨论的升列是不可约升列时, 结论才是定理 一般 成立的充分且必要条件. 由于以上升列 HYP 不是不可约的, 从而引起了以上程序的失败.

HYP 可约的原因是在于直线与圆相交的歧义性, 以致于点对 A_1, A_1' 和 A_2, A_2' 不能被区分. 这就要用前一节中的方法或把升列 HYP 分解为不可约形式. 从 H_3 减去 H_1 得到

$$H_3' = H_{31}' * H_{32}',$$

这里

$$H_{31}' = x_1' - x_1, \quad H_{32}' = (a_1^2 + b_1^2) * (x_1' + x_1) + 2 * a_1 * (b_1 * y_0 - a_1 * x_0).$$

相似地, 从 H_7 减去 H_7 有

$$H_7' = H_{71}' * H_{72}',$$

这里

$$H_{71}' = x_2' - x_2, \quad H_{72}' = (a_1^2 + b_1^2) * (x_2' + x_2) + 2 * a_1 * (b_1 * y_0 - a_1 * x_0).$$

于是

$$\text{Zero}(HYP) = \bigcup_{i=1,\cdots,4} \text{Zero}(HYP_i),$$

其中 HYP_i 是不可约升列:

$$\left.\begin{aligned}
HYP_1 &= \{H_1, H_2, H_{31}', H_4, H_5, H_6, H_{71}', H_8, H_9, H_{10}, H_{11}, H_{12}\}, \\
HYP_2 &= \{H_1, H_2, H_{31}', H_4, H_5, H_6, H_{72}', H_8, H_9, H_{10}, H_{11}, H_{12}\}, \\
HYP_3 &= \{H_1, H_2, H_{32}', H_4, H_5, H_6, H_{71}', H_8, H_9, H_{10}, H_{11}, H_{12}\}, \\
HYP_4 &= \{H_1, H_2, H_{32}', H_4, H_5, H_6, H_{72}', H_8, H_9, H_{10}, H_{11}, H_{12}\}.
\end{aligned}\right\} \tag{7.3.82}$$

容易证明

$$\text{Remdr}(CONC/HYP_i) \neq 0,\ i = 1, 2, 3,$$

$$\text{Remdr}(CONC/HYP_4) = 0.$$

令 IP_i 为 $HYP_i (i = 1, \cdots, 4)$ 的初式积，其中 HYP_i 是不可约升列．由机械化定理证明原理 II, 割线定理仅在 $\text{Zero}(HYP_4/IP_4)$ 上成立，而在其余 3 部分 $\text{Zero}(HYP_i/IP_i)(i = 1, 2, 3)$ 上不成立．我们也可以用机械化定理证明原理 III 看到割线定理在整个 $\text{Var}[HYP_4]$ 上是正确的，而在其他 3 个簇不成立．其几何意义是相当明显的．

注释 7.3.15 通过对几何实体的精心安排,割线定理可以转化为一种 Hilbert 型，从而用 §7.2 中的方法证明．

注释 7.3.16 有各种特殊的策略可以处理常用几何定理中的歧义性．不仅上一节的各种定理，即 Feuerbach 定理，Morley 定理，Steiner 定理，可以用上面描述的机械化定理证明原理详细地证明和分析，而且一些更棘手的定理，如 Thébault-Taylor-Chou 定理也可以用相同的方法处理．可是，由于我们在这里主要是对几何定理证明的一般原理，而不是定理本身感兴趣，我们把这些主题放在由 Chou, Gao, Wang, Wu 等的原始文献中．

§7.4 涉及不等式的几何定理机器证明

实数域上的不等方程和不等式

在这一节基域 **K** 为实数域 **R**. 尽管我们的思想可以推广到一般的实闭域，但是我们仍限制在域 **R** 上，以避免任何肤浅的推广．

根据 Seidenberg, 可以把不等方程和不等式归结为某些关于 y 多项式的解的存在性．这在引理和以下例子中有所说明．

引理 7.4.1 设 a, b, c 为常数， y 是 **R** 上的未定元，那么:

$$\begin{aligned}
a > 0 \quad &\Longleftrightarrow \text{Zero}_{\mathbf{R}}(a * y^2 - 1) \neq \emptyset,\\
a < 0 \quad &\Longleftrightarrow \text{Zero}_{\mathbf{R}}(a * y^2 + 1) \neq \emptyset,\\
a \geq 0 \quad &\Longleftrightarrow \text{Zero}_{\mathbf{R}}(y^2 - a) \neq \emptyset,\\
a \leq 0 \quad &\Longleftrightarrow \text{Zero}_{\mathbf{R}}(y^2 + a) \neq \emptyset,\\
a \neq 0 \quad &\Longleftrightarrow \text{Zero}_{\mathbf{R}}(a * y - 1) \neq \emptyset,\\
a, b\ \text{同号} \quad &\Longleftrightarrow \text{Zero}_{\mathbf{R}}(a * b * y^2 - 1) \neq \emptyset,\\
a, b\ \text{异号} \quad &\Longleftrightarrow \text{Zero}_{\mathbf{R}}(a * b * y^2 + 1) \neq \emptyset,
\end{aligned}$$

$$c \text{ 在 } a,b \text{ 之间} \iff \mathrm{Zero}_{\mathbf{R}}(b-c)*(c-a)*y^2-1) \neq \emptyset,\ (a \neq b),$$
$$c \text{ 不在 } a,b \text{ 之间} \iff \mathrm{Zero}_{\mathbf{R}}(b-c)*(c-a)*y^2+1) \neq \emptyset,\ (a \neq b)$$

例 7.4.2 对于在实平面上位于同一直线的互异的三点

$$A_1 = (a_1, a_4), \quad A_2 = (a_2, a_5), \quad A_3 = (a_3, a_6),$$

A_2 位于 A_1, A_3 之间当且仅当

$$\mathrm{Zero}_{\mathbf{R}}((a_2-a_1)*(a_2-a_3)*y^2+1)+\mathrm{Zero}_{\mathbf{R}}((a_5-a_4)*(a_5-a_6)*y^2+1) \neq \emptyset.$$

例 7.4.3 实平面 $\mathbf{R}^2(x_1, x_2)$ 中两点 $A = (a_1, a_2)$, $A' = (a_1', a_2')$ 位于上直线

$$L(x_1, x_2) \equiv c_1 * x_1 + c_2 * x_2 + c_0 = 0$$

(c_1, c_2 不全为零) 同侧或不同侧分别等价于

$$\mathrm{Zero}_{\mathbf{R}}(L(a_1, a_2) * L(a_1', a_2') * y^2 - 1) \neq \emptyset,$$

或

$$\mathrm{Zero}_{\mathbf{R}}(L(a_1, a_2) * L(a_1', a_2') * y^2 + 1) \neq \emptyset.$$

<u>范围 T 上的几何定理证明</u>

令 $X = (x_1, \cdots, x_n)$. 在 Tarski 域 **T** 上考虑定理 T. 在通常的确切意义上考虑几何概念, T 的假设和结论都可表示为关于变量 X 由逻辑符号 $\exists, \forall, \wedge, \vee, \neg$ 连接的多项式等式、不等式的集合. 通过消元, Tarski 给出了证明或否定域 **T** 上任何这种定理的一般步骤, 看 Tarski 定理. 我们可以把这个定理转换为以下形式:

Tarski 定理. 域 **T** 上的几何定理是 可机械化.

Tarski 的算法很复杂, 以致于很难证明几何中有意义的定理. Tarski 的方法被后来的研究者作了极大的改进. 其中最成功的有 Collins 的 CAD(柱状代数分解) 方法. 到目前为止, CAD 方法已产生了许多有几何和数学意义的结果, 并正在得到更近一步的改进.

Tarski 和 Collins 算法的高复杂性来源于两个方面. 首先, 他们在很一般的特征下考虑问题; 例如: 实闭域上的可决定性问题. 其次, 对于所考虑的几何定理, 几何概念是对实际的几何意义上而言的, 它们的代数等价表达式非常复杂, 参见 §7.1. 为了减少这个方法的复杂度而增加它的有效性, 在牺牲一般性和完备性的情况下, 我们采用下面的方法.

自然地, 我们在较窄的应用范围下考虑. 对于几何问题, 我们适当调整几何概念, 以便如 7.1 节解释的一样使它们有相当简单的代数等价表达式. 现在

在这种理解下，我们考虑范围 $\mathbf{T}$ 的定理 T, 其假设和结论均可由 $\vee, \wedge, \neg$ 连接的多项式方程、不等方程、不等式表示，所有的多项式都在 $\mathbf{R}[X]$ 中. 用引理 7.4.1 中的 Seidenberg 方法，必要时加入新变量 $Y=(y_1, \cdots, y_m)$, 就可以把假设转化为 $HYP=0$ 的形式，其中 HYP 是 $\mathbf{R}[X,Y]$ 中的多项式集，也可能最终是某些简单的不等方程和不等式. 不失去更多一般性，我们仅考虑结论一般形式为 $CONC=0, \neq 0, >0, <0, \geq 0$, 或 ≤ 0 的情形，其中多项式 $CONC$z 在 $\mathbf{R}[X,Y]$ 中. 注意: HYP 中新变元 Y 的存在性由假设本身暗示. 我们把定理表示为 $T=\{HYP, CONC, \mapsto\}$, 其中 $\mapsto$ 代表 $=, \neq, >, <, \geq$, 或 $\leq$, 表示定理 T 的结论为 $CONC \mapsto 0$. 现在我们用引理 7.4.1 把结论转化为 $CONC'=0$ 的形式. 如果必要的话，可加入新变元 y_0, 其中 $CONC'$ 在 $\mathbf{R}[X,Y,y_0]$ 上. 可是，与假设的情形不同，新变元 y_0 的存在不再由结论或定理本身暗示，而是将要证明的. 因此，把结论转化为一个方程在这里一点也没有优势，为此，我们将限制引入任何新变元. 把 X, Y 重新记为 X, 在范围 $\mathbf{T}$ 中限制的范围 $\mathbf{T}'$ 中，我们把几何定理证明描述如下：

定义 7.4.4 $\mathbf{T}'$ 是指几何定理 $T=\{HYP, CONC, \mapsto\}$ 的范围，其中 $T=\{HYP, CONC, \mapsto\}$, $CONC$ 在 $\mathbf{R}[X]$ 中， $\mapsto$ 代表 $=, \neq, >, <, \geq$, 或 $\leq$. HYP 是指 T 的假设多项式集, $CONC$ 代表 T 的结论多项式.

定义 7.4.5 对于在 $\mathbf{T}'$ 上的定理 $T=\{HYP, CONC, \mapsto\}$, 定理的假设是指 $HYP=0$, 结论是指 $CONC \mapsto 0$.

问题 $\mathbf{T}'$ 寻找一种一般的方法，使得在有限步内决定 $\mathbf{T}'$ 上定理 $T=\{HYP, CONC, \mapsto\}$ 的假设 $CONC \mapsto 0$ 是否是 HYP 的结果.

注释 7.4.6 对于 $\mathbf{T}'$ 上定理，有时保留一些简单的不等式而不引入新变元 y_i 会带来方便. 这要求我们忽略某些不感兴趣或不合理的退化情形.

在限制范围 $\mathbf{T}'$ 上几何定理的证明

考虑范围 $\mathbf{T}'$ 上定理 $T=\{HYP, CONC, \mapsto\}$. 如果 $\mapsto$ 代表 $=$, 那么定理 T 仍然是在范围 $\mathbf{E}$ 上，于是可以采取 §7.2 中描述的任何一种机械化定理证明原理. 于是，就可以只考虑这样的定理 $T=\{HYP, CONC, \mapsto\} \in \mathbf{T}' \setminus \mathbf{E}$, 其中 $\mapsto$ 表示 $\neq, >, <, \geq$ 或 $\leq$, 但不包含 $=$. 我们应用另一种修改形式的机械化定理证明原理.

例如，考虑机械化定理证明原理 I. CS 是 $HYP \subset \mathbf{R}[X]$ 的特征集, I_i 是 CS 中 C_i 的初式. 由 §3.3, 我们可以使 $CONC$ 关于 CS 的平方余式 R 有这样的形式：

$$(\Pi_i\ I_i^{2*s_i}) * CONC = \sum_i Q_i * C_i + R, \tag{7.4.83}$$

其中 Q_i, R 位于 $\mathbf{R}[X]$, R 关于 CS 约化，s_i 为非负整数. 为了证明 $CONC \mapsto 0$, 则只要在条件 $C_i = 0$ 下，有

$$R \mapsto 0.$$

有时这样就比直接从假设 $HYP = 0$ 证明结论 $CONC \mapsto 0$ 要更容易. 其余的机械化定理证明原理可以同样地应用. 因此，这种方法可以用来证明 $\mathbf{T}'$ 中的定理. 尽管它一点也不完备的，但能部分地取得成功.

例 7.4.7 (Pasch 定理) 给定三角形 ABC, 直线 L 不过任一顶点，分别交三边 BC, AC, AB 于 D, E, F. 那么 D, E, F 中或者只有两点，或者没有点位于线段 BC, AC, AB 上.

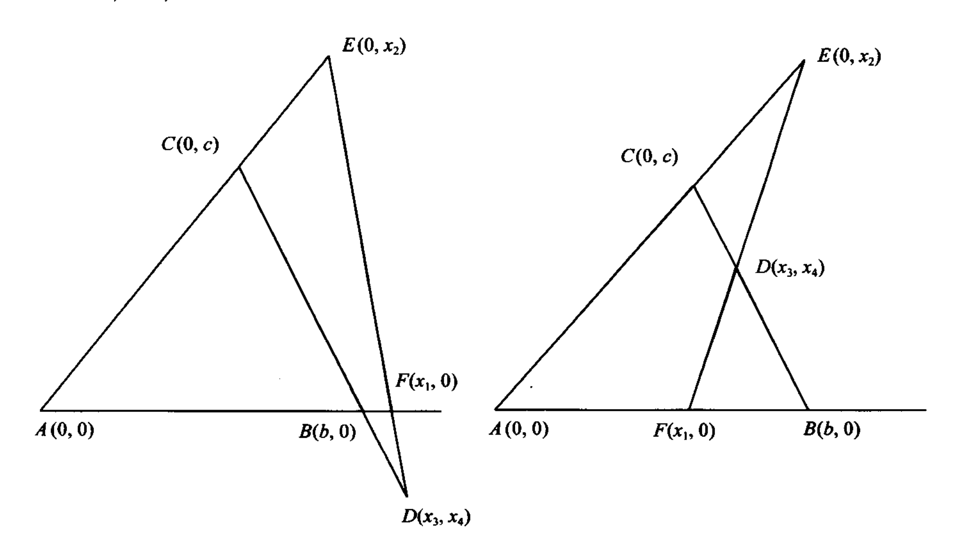


图 7.11 Pasch 定理

证明 假定 E, F 分别同时位于线段 AC, AB 上，或同时位于线段 AC, AB 外. 要证明 D 位于线段 BC 外. 另一种情形可以利用反证法由这一情形导出.

为此，我们取斜坐标：

$$\begin{aligned} &A = (0,0), \quad B = (b,0), \quad C = (0,c), \\ &F = (x_1,0), \quad E = (0,x_2), \quad D = (x_3,x_4), \end{aligned} \tag{7.4.84}$$

其中 $b \neq 0, c \neq 0$. 由引理 7.4.1, 对于 y_1, y_2 有假设集 $HYP = \{H_1, H_2, H_3, H_4\}$,

其中

$$\left.\begin{aligned}H_1&=y_1^2*x_1*(b-x_1)+e,\\H_2&=y_2^2*x_2*(c-x_2)+e,\\H_3&=x_3*(b*x_2-c*x_1)-b*x_1*(x_2-c),\\H_4&=x_4*(b*x_2-c*x_1)+c*x_2*(x_1-b).\end{aligned}\right\}\tag{7.4.85}$$

在 (7.4.85) 中 e 是 -1 或 $+1$, 分别对应于 E,F 在 AC,AB 外或在 AC,AB 内. 结论多项式为

$$CONC=x_3*(b-x_3),$$

我们要证

$$x_3*(b-x_3)<0.$$

取序为

$$y_1\prec y_2\prec x_1\prec x_2\prec x_3\prec x_4,$$

这样 HYP 已经是升列形式并且本身是 HYP 的一个特征集. $CONC$ 的平方余式公式为

$$y_1^4*y_2^4*(b*x_2-c*x_1)^2*CONC\equiv-b^2*y_1^2*y_2^2 \mod HYP,$$

因此平方余式为

$$-b^2*y_1^2*y_2^2<0,$$

于是 $CONC<0$ 得到证明. □

实 8-3 元组构形

例 7.4.8 (修改的例 7.3.1) 从例 7.3.1 的证明可见, 在复仿射空间存在 ∞^8 非平凡 8-3 元组构形. 相反 S. C. Chou 和 X. S. Gao 发现并证明了以下漂亮的定理 (参见 [C-G2]).

定理 7.4.9 在实仿射空间不存在非平凡 8-3 元组构形.

证明 设 $\{A_1,\cdots,A_8\}$ 是非平凡 8-3 元组构形, 其中 A_i 由 (7.3.55) 给定, 并满足 (7.3.56) 中的 $P_j=0,j=1,\cdots,7$. 从 8-3 元组定理的证明知, 我们知道 $y_3\neq0$ 成立. 我们应该有 $y_5\neq0$, 否则从 $P_1=0$ 就有 $x_5=x_2$ 或 $A_5=A_2$. 相似地, 从 $P_2=0,P_3=0,P_7=0$, 我们应该分别有 $y_6\neq0,y_7\neq0$, 和 $y_8\neq0$. 另外为了得到 $A_4\neq A_2$, 我们还要有 $x_2\neq0,x_4\neq0$ 和 $x_4\neq x_2$. 从而

$$NZ\equiv y_3*y_5*y_6*y_7*y_8*x_4*x_2*(x_4-x_2)\neq0.$$

取与 (7.3.57) 中相反的变量序, 则由 wsolve 我们把 $\mathrm{Zero}(HYP/NZ)$ 分解为 10 个分支, 其升列为 $AS_j, j = 1, \cdots, 10$, 初式积为 IP_j, 使得

$$\mathrm{Zero}(HYP/NZ) = \bigcup_j \mathrm{Zero}(AS_j/IP_j * NZ).$$

在这 10 个升列中, 有 4 个将导致 8 个点 A_i 中有两点重合, 必须舍弃. 在其余 6 个升列中, 只有一个多项式关于主变元是二次的, 其余多项式关于主变元都是线性的. 例如, 这样的一个二次多项式有以下形式:

$$P = y_3^2 * (3 * y_7^2 - 3 * y_7 * y_8 + y_8^2) - y_3 * y_7 * y_8 * (3 * y_7 - y_8) + y_7^2 * y_8^2.$$

P 关于 y_3 的结式为

$$-3 * y_7^2 * y_8^2 * (y_7 - y_8)^2 < 0.$$

这样, 因为 $y_7 \neq y_8$, 否则 $P_6 = 0$ 将导致 $x_7 = x_8$, 所以 $A_7 = A_8$. 于是对应的升列没有实零点, 其他 5 个升列有相似的讨论. 这就证明了 HYP 没有实零点, 从而 $NZ \neq 0$. 因此定理得证. □

<u>角平分线相等的三角形</u>

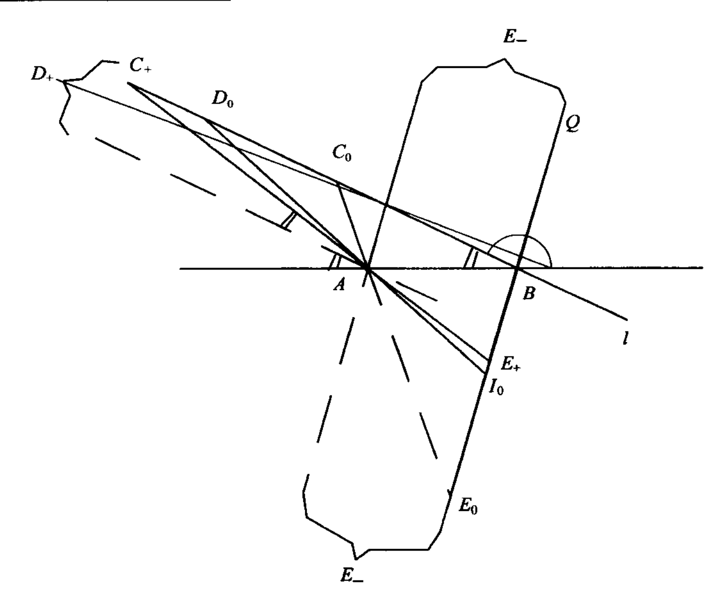


图 7.12 角平分线相等的三角形

关于有相等角平分线的三角形的诡辩问题曾困扰了 19 世纪的几何学家. 对于等腰三角形 ABC, $|AC| = |BC|$, 容易证明角 A,B 的内角平分线相等. 但

是，其真逆命题却不是很容易地用通常的 Euclid 方式证明. 而且，如果有一条角平分线在外部，那么很可能两角平分线相等但对应边 $|AC|$ 和 $|BC|$ 不相等. 为了看到这一点，举例来说，我们考虑角 A, B 的平分线 AD, BE 在外部. 把顶点 A, B 和直线 $l = BC$ 固定，顶点 C 沿固定直线 l 移动. 角 B 的外角平分线仍然是固定直线 m. 我们过 A 点作直线与 m 平行交 l 于点 C_-. 对于 $C = C_-$，角 B 的外角平分线 BE_- 的终点会成为无穷远点，从而 $|BE_-| = +\infty$. 所以对于角 A 的外角平分线 AD_-，我们有 $|AD_-| < |BE_-|$. 过 A 作直线与 l 平行，作关于这条直线与直线 AB 反射的直线，交 l 与点 C_+. 那么，对于三角形 ABC_+，角 A 的外角平分线 AD_+ 与 l 平行，D_+ 为 l 上的无穷远点. 因此 $|AD_+| = +\infty$，于是在 $C = C_+$ 的情形下，对于这两个外角平分线有 $|AD_+| > |BE_+|$. 那么，当顶点 C 沿直线 l 从 C_- 移动到 C_+ 时，将会在某个位置 C_0 使角 A, B 的外角平分线 AD_0, BE_0 等长. 对于这样的三角形，两外角平分线相等，但对应的两边却不等. 当顶点 B 固定时，直线 l 可以变化，因此像以上的反例有无穷多，参见图 7.12.

当两个角平分线一个为内角平分线，一个为外角平分线时，相似的情形也会出现. 当然，两个角平分线在内部时，情况就完全不同了. 事实上我们有以下定理：

例 7.4.10 (相等角平分线定理) 如果三角形的两内角平分线相等，那么对应的两边相等. 另一方面，如果这两个角平分线不都在内部，将有无穷多个三角形有相等的角平分线，但其对应边不相等.

证明 设三角形 ABC 的两个角 A 和 B 的角平分线为 AD, BE(在三角形的内部或外部)，在内心或外心 I 处相交，并且长度相等. 我们取坐标为

$$\left.\begin{array}{lll} A = (-x_1, 0), & B = (+x_1, 0), & I = (x_2, x_3), \\ C = (x_4, x_5), & D = (x_6, x_7), & E = (x_8, x_9). \end{array}\right\} \tag{7.4.86}$$

假设多项式集 $HYP = \{H_i \mid i = 1, \cdots, 7\}$，其中 $H_7 = |AD|^2 - |BE|^2$ 和

$$\left.\begin{array}{ll} H_1 = & x_4 * (x_3^2 + x_2^2 - x_1^2) + 2 * x_2 * (x_3^2 - x_2^2 + x_1^2), \\ H_2 = & x_5 * (x_3^2 + x_2^2 - x_1^2) - 2 * x_3 * (x_2^2 - x_1^2) \text{等} \end{array}\right\} \tag{7.4.87}$$

设 HYP 的特征集为 $CS = \{C_i \mid i = 1, \cdots, 7\}$，其中

$$\left.\begin{array}{l} C_1 = x_2 * C_1', \\ \text{其中} \\ C_1' = (x_3^2 + x_2^2 - x_1^2)^2 * (x_3^2 + 2 * (x_2^2 - x_1^2)) \\ \qquad -4 * x_1^2 * (x_2^2 - x_1^2)^2. \end{array}\right\} \tag{7.4.88}$$

为了说明 $C_1=0$ 是不是 $HYP=0$ 的结论，我们需要证明 $x_2=0$ 或 $C_1'=0$. 我们注意到，现在还没有考虑角平分线 AD 和 BE 是否在内部或外部. 我们假定 $x_1>0, x_5>0$, 于是 A 位于 X 轴上 B 的左侧，而 C 位于 Y 轴的上面. 现在角平分线 AD 是否在内部取决于 AI 的斜率 $\frac{x_3}{x_2+x_1}=e_1>0$ 或 <0. 类似地，角平分线 BE 是否在内部取决于 BE 的斜率 $\frac{x_3}{x_2-x_1}=-e_2<0$ 或 >0. 特别地，$x_2^2-x_1^2$ 与 $-e_1*e_2$ 有相同的符号，并且

$$\frac{x_3^2}{x_2^2-x_1^2}=-e_1*e_2. \tag{7.4.89}$$

如果 $e_1*e_2<0$, 那么两条分角线一条在内部，另一条在外部. 另一方面，设 $e_1*e_2>0$, 那么 AD, BE 都在内部或外部取决于 I 和 C 是否同时在 X 轴的一边，即 $x_3*x_5>0$ 或 $x_3*x_5<0$. 由 (7.4.87) 中 H_2, 我们有

$$x_3*x_5=\frac{2*x_3^2}{1-e_1*e_2}.$$

从而，角平分线 AI, BI 同时在内部或外部取决于 $0<e_1*e_2<1$ 或 $e_1*e_2>1$.

首先考虑 $e_1*e_2>0$ 的情形. 由 (7.4.88) 和 (7.4.89) 我们有

$$C_1'=(x_2^2-x_1^2)^3*\left((1-e_1*e_2)^2*(2-e_1*e_2)-\frac{4*x_1^2}{x_2^2-x_1^2}\right). \tag{7.4.90}$$

先假定 $0<e_1*e_2<1$, 使得两个分角线都在内部. 这样 $x_2^2-x_1^2<0$, 从 (7.4.90) 可以看出 C_1' 总是为负的. 于是 $C_1'\neq 0$, 并且从 $C_1=0$ 必定有 $x_2=0$. 这说明三角形是等腰的，从而定理的第一部分得证.

其次假定 $e_1*e_2>1$, 于是两个分角线都在内部或外部. 从 (7.4.88) 我们知道，存在无穷多非等腰三角形，具有相等的外角平分线. 事实上，将 (X,Y) 作为活动坐标，外心 $I=(x_2,x_3)$ 将描出一个次数为 6 的椭圆形曲线，其方程为

$$Y^6+4*Y^4*(X^2-a^2)+5*Y^2*(X^2-a^2)^2+2*(X^2-a^2)^3\ =4*a^2*(X^2-a^2)^2,$$

其中 $x_1=a$ 是一个正常数，则我们知道该曲线达到过 A,B 的垂线，并且其高度比 AB 上的等边三角形要略低. 见图 7.13.

当 $e_1*e_2<0$ 时，一条角平分线在内部，另一条在外部，这种情形可以类似处理. 此时存在无限个非等腰的三角形使得其一条内角平分线和外角平分线相等. 对应的外切圆圆心 $I=(x_2,x_3)$ 将描出两个次数为 6 的椭圆形曲线，分别达到过 A,B 的两条垂线，并且这两条垂线分别通过点 $(+\sqrt{3}*x_1,0)$ 和 $(-\sqrt{3}*x_1,0)$. 这些卵形曲线的高度略小于其宽度. 参见图 7.13. □

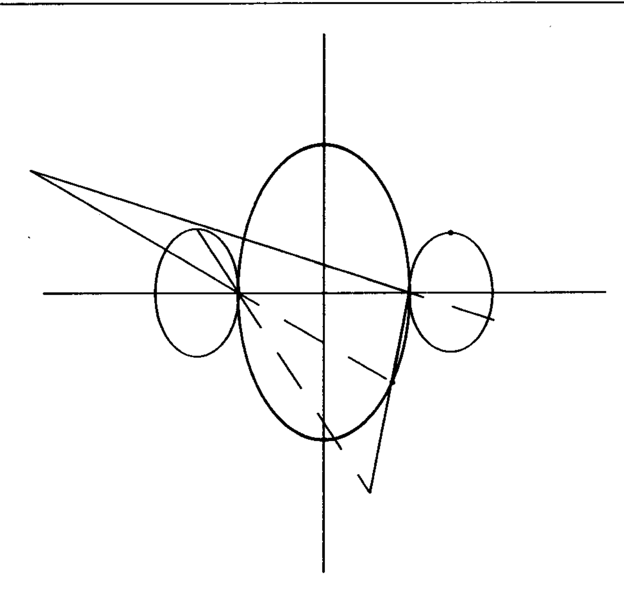


图 7.13 相等角平分线定理

注释 7.4.11 以上结果是 S. C. Chou, X. L. Lu, 和本书作者讨论的结果. 图 7.13 为 X. L. Lu 所作.

在范围 $\mathbf{T}'$ 上定理证明的另一种方法

§5.5 中的有限性定理可以应用到范围 $\mathbf{T}'$ 上的定理证明. 以下给出例子说明这种应用.

例 7.4.12 (修改的 Pasch 定理) 对于三角形 ABC, 一直线分别交三边 BC, AC, AB 于 $D, E, F(D, E, F$ 与顶点不同). 假定 D 在线段 BC 内部, E 在线段 AC 外部 (序为 ACE). 要证明 F 在 AB 内部.

和 (7.4.84) 类似, 取坐标使

$$\begin{aligned} &b > 0, \quad c > 0, \quad x_2 > c, \\ &0 < x_3 < b, \quad 0 < x_4 < c. \end{aligned} \tag{7.4.91}$$

现在不考虑 D 为开放线段 BC 上的定点, 而是考虑为闭线段 BC 上的活动点, 我们让 x_3, x_4 在闭域

$$\bar{D}: 0 \le x_3 \le b \quad (\text{或 } 0 \le x_4 \le c) \tag{7.4.92}$$

上变动. 由 D, E, F 共线, 我们有 $H_1 = 0, H_2 = 0$, 其中

$$\left.\begin{aligned} H_1 &= x_3 * (b * x_2 - c * x_1) - b * x_1 * (x_2 - c), \\ H_2 &= x_4 * (b * x_2 - c * x_1) + c * x_2 * (x_1 - b). \end{aligned}\right\} \tag{7.4.93}$$

我们取变量序为

$$x_1 \prec x_3 \prec x_4,$$

注意 $x_2(>c)$ 固定. 现在问题是要决定在约束方程 $H_1=0, H_2=0$ 下，对于 x_3, x_4 在闭域 $\bar{D}$ 上变动时 x_1 的最小值和最大值的明显存在. 因此变量 x_1 取到 5.5 节有限核定理中 x_0 的作用. 为此，我们把区域 $\bar{D}$ 在分别的反射空间分为 3 个开放区域 O_1, O_2, O_3, 其中 O_1 由 (7.4.91) 定义, O_2, O_3 分别由 $x_3=0$ 和 $x_3=b$ 定义. 对于 O_2 有 $x_1=0$, 对于 O_3, 有 $x_1=b$, 分别为点 $(x_3,x_4)=(0,c)$ 和 $(b,0)$ 在 x_1 上的投影. 对于 O_2 和 O_3, 核集为

$$K_2=\{0\}, \quad K_3=\{b\}. \tag{7.4.94}$$

另一方面, O_1 的核集容易知道为

$$K_1=\emptyset. \tag{7.4.95}$$

(7.4.94) 和 (7.4.95) 给出这个问题的核集为

$$K=K_1+K_2+K_3=\{0,b\}\subset \mathbf{R}.$$

于是，对于位置 $F=A, D=C$ 和 $F=B, D=B$, x_1 分别取最大值和最小值. 对于 $D\neq C,B$, 即对于 D 在 BC 内部，必须有 $0<x_1<b$ 或 F 在 AB 内部. □

注释 7.4.13 这个证明看起来过于复杂，然而，这是对这样一种普遍原理的一个简单说明，这个原理可把范围 $\mathbf{T}'$ 上的定理证明归结为一个最优化问题，从而可以用 5.5 节中的方法解决. 事实上，一些相当难的定理已经用这样的方法证明. 参见作者关于不等式的适当的论文. 为了说明这个原理，我们在下面进一步给出例子.

例 7.4.14 (四边形凸性定理)　$ABCD$ 为凸四边形，点 O,P,Q,R 分别在 AD, AB, BC 和 CD 内部，那么 $OPQR$ 也是凸四边形.

证明　由于 $ABCD$ 的凸性，斜坐标可取为

$$O=(0,0),\quad A=(0,-a),\quad B=(b_1,-b_2),\quad C=(c_1,c_2),\quad D=(0,d),$$

$$Q=(q,0),\quad q=\frac{b_1*c_2+b_2*c_1}{b_2+c_2},$$

$$P=r_0*B+(1-r_0),\quad A=(r_0*b_1,\quad -r_0*b_2-(1-r_0)*a),\quad 0<r_0<1,$$
$$R=r*C+(1-r),\quad D=(r*c_1,r*c_2+(1-r)*d),\quad 0<r<1,$$

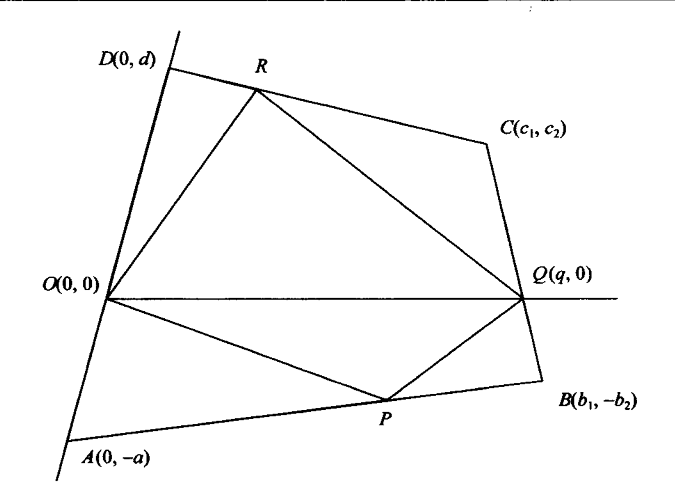


图 7.14 四边形凸性定理

常数 a, b_1, b_2, c_1, c_2, d 都为正数，于是 q 也为正．令

$$k = \frac{(\triangle OQR)\text{的有向面积}}{(\triangle OQP)\text{的有向面积}},$$

使得 $H = 0$, 其中

$$H = k * (r_0 * b_2 + (1 - r_0) * a) + (r * c_2 + (1 - r) * d).$$

要证明 $k < 0$ 或 R, P 在直线 OQ 的两侧．为此，和例 7.4.12 相似，把 R 看成闭线段 CD 上的活动点，r 在闭域 $\bar{D}$ 上变动，其中

$$\bar{D} : 0 \le r \le 1.$$

把 r_0 看成常数，取变量序为

$$k \prec r.$$

接着处理关于 k 在限制 $H = 0$ 下域 $\bar{D}$ 上的最优化问题．这里 k 的地位与 §5.5 有限核定理中的 x_0 类似．把域 $\bar{D}$ 分为 O_1, O_2, O_3, 分别对应与 $0 < r < 1, r = 0$, 和 $r = 1$.

首先假定 $c_2 \ne d$ 或 CD 不与 OQ 平行．于是 O_i 和 $\bar{D}$ 的核集分别为 (Proj_k 表示在坐标 k 上的投影)

$$K_1 = \emptyset,$$

$$
\begin{aligned}
K_2 &= \{k_2\} = \mathrm{Proj}_k \ \{(k,r) = (k_2,0)\}, \\
K_3 &= \{k_3\} = \mathrm{Proj}_k \ \{(k,r) = (k_3,1)\}, \\
K \ &= \ K_1 + K_2 + K_3 = \{k_2, k_3\},
\end{aligned}
$$

其中

$$
k_2 = -\frac{d}{r_0 * b_2 + (1 - r_0) * a} < 0,
$$

$$
k_3 = -\frac{c_2}{r_0 * b_2 + (1 - r_0) * a} < 0.
$$

因此我们看到 k 的最大值和最小值都是负数. 如果 $c_2 = d$, 那么 k 的最大值和最小值都等于相等的负数 $k_2 = k_3$. 无论如何我们有 $k < 0$. 从而 R, P 在直线 OQ 的两侧. 相似地可证, O, Q 在直线 PR 两侧. 所以四边形 $OPQR$ 是凸的. □

相等角平分线定理的另一种证明

例 7.4.15 (修改的相等角平分线定理) 我们再考虑相等角平分线定理. 以下将用基于 §5.5 中有限核定理的方法证明定理的第一部分. 和前面一样, 我们假定 $x_5 > 0, x_1 = a_1 > 0$ 是正常数, 且 $e_1 > 0, e_2 > 0$, 于是 AD, BE 都是内角平分线. 也取 $x_3 = a_3 > 0$ 为正常数. 这样就一定有 $a_1 > a_3$, 保证了上面假设的有效性.

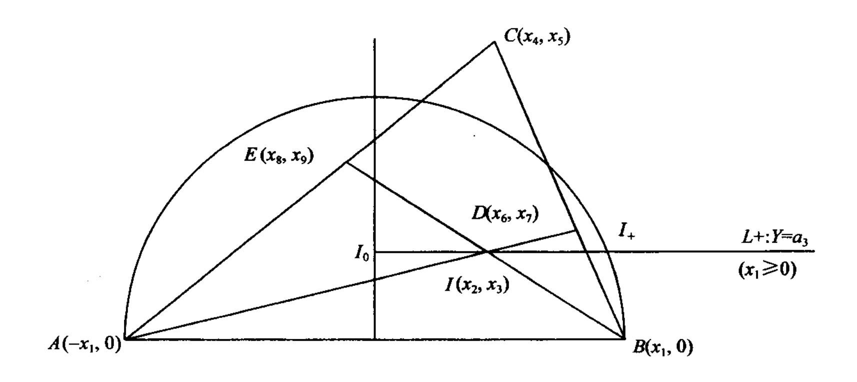


图 7.15 修改的相等角平分线定理

我们考虑 I 不是一个固定点, 而是把 I 看成在半直线上的活动点:

$$
\begin{aligned}
L_+ &: \ X \geq 0, \ \ Y = a_3, \\
L_- &: \ X \leq 0, \ \ Y = a_3.
\end{aligned}
$$

以 AB 为直径在上半平面作半圆，分别交半直线 L_+ 和 L_- 于点 $I_+ = (a_2, a_3)$ 和 $I_- = (-a_2, a_3)$, 其中 $a_2 = +\sqrt{a_1^2 - a_3^2} > 0$. 为了保证 I 在三角形内部，限制 I 在闭直线 I_0I_+ 上变动，其中 $I_0 = (0, a_3)$, 见图 7.15. 注意，对于 $I = I_+$ 或 $I = I_-$, 边 AC, BC 将互相平行，因此 C 成为无穷远点，这样 ABC 就不再是真正意义上所说的三角形了. 可是这对我们的方法没有影响. 因为我们可以忽略顶点 C, 把图形限制为只由点 A, B, I, D, E 构成.

考虑 (7.4.87) 中的假设多项式 H_i. 对于我们的假设，我们引入新变量 x_0, 把 H_7 换成 $H_7' = H_7 - x_0$, HYP 换成 $HYP' = \{H_3, \cdots, H_6, H_7'\}$. 作为定理证明的第一步，当 I 取遍闭区间 I_0I_+ 时，我们将决定 x_0 在约束条件 $HYP' = 0$ 下的极小值， 和前面的例子类似，我们把闭区间分为：$0 < x_2 < a_2$, I_0 和 I_+. 对于第一部分，核集为 $K_1 = \emptyset$, 对于其他两个，核集分别为 $K_2 = \{0\}$ 和 $K_3 = \{16 * a_1 * a_2\}$, 其中 $a_1 * a_2 > 0$. 从而，当 I 在闭区间 I_0I_+ 上移动时，当且仅当 $I = I_0$, x_0 的最小值取到 0. 这样三角形是等腰的. 相似地，当 I 在闭区间 I_0I_- 上移动时，当且仅当 $I = I_0$, x_0 取到最大值 0, 即当且仅当三角形为等腰三角形. 这样，当 I 在闭区间 I_-I_+ 上移动时，只有当三角形 ABC 为等腰三角形时， $|x_0|$ 能取到最小值. 对于任意固定的 $x_3 = a_3 > 0$, 相同的事实也成立. 从而，当且仅当三角形 ABC 是等腰三角形时，对于 I 在上半平面变动并保持 I 是三角形的内心， $|x_0|$ 能取到最小值 0. □

<u>Euler 不等式</u>

例 7.4.16 (Euler 不等式) 定理：令 $r(>0)$ 和 $R(>0)$ 分别为三角形 ABC 的内切圆和外接圆的半径，则 Euler 比例 $E = \frac{r}{R}$ 小于或等于 $\frac{1}{2}$. 仅当三角形 ABC 为等边三角形时，E 达到最大值 $\frac{1}{2}$.

证明 明显地，我们可把证明归结为下列优化问题：对于作为变元的三角形 ABC, 求 Euler 比例的最大值. 我们首先考虑一个固定三角形 ABC, 设 AB 的中点为 M, 外接圆的中心为 O, 设过 M 与 AB 垂直的直线与圆弧 ACB 交于 C_0. 令 I_0, I 分别为三角形 AC_0B 和 ACB 的内心，则 I_0 显然是弧 AIB 的中点， I, I_0, C, C_0 都在直线 AB 的同侧. 见图 7.16.

我们把点 C 看成弧 AC_0B 上的动点，而不是一个定点，则内心 I 为弧 AI_0B 上的动点. 显然，变元三角形 ABC 的内切圆的半径有最大值 $r_0 = |OI_0|$, 而它的外接圆的半径保持为 R. 于是，当 C 沿弧 AC_0B 上运动时，Euler 比例当 C 在 C_0 位置时取得最大值 $E_0 = \frac{r_0}{R}$. 于是，如果我们把 A, B 看作定点，而 C_0 看作过点 M 垂直于 AB 的射线上的动点时，则问题归结为决定最终 $E_0 = \frac{r_0}{R}$

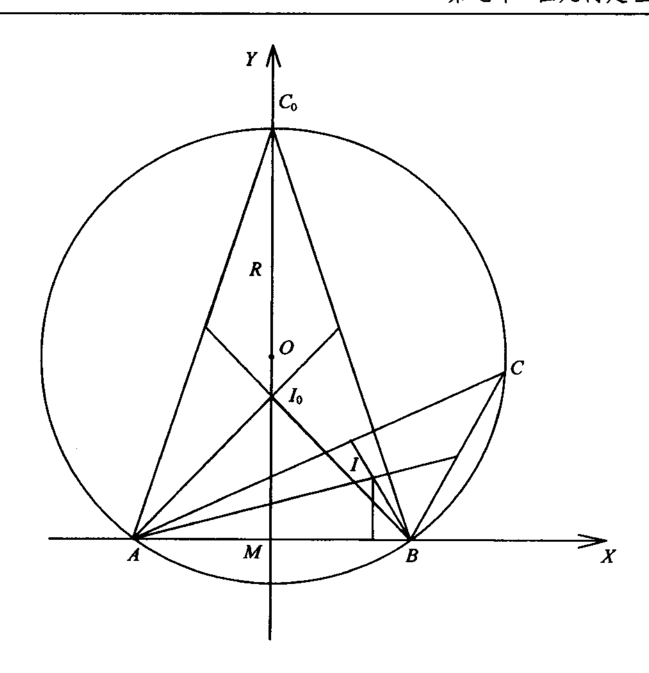


图 7.16 Euler 不等式

的最大值，该值仅依赖于 AB.

为此，我们考虑以 M 为原点的坐标系 (x, y), 其中, MB 为 x 轴的正向, MC_0 为 y 轴的正向. 设 $A = (-a, 0)$, $B = (a, 0)$, $O = (0, b)$, 则 $C_0 = (0, R + b)$, $I_0 = (0, r_0)$, 其中 $a > 0$, $R + b > 0$, $r_0 > 0$. 因此, C_0 和 I_0 与 M 不同. 我们得到

$$h_1 \equiv R^2 - (a^2 + b^2) = 0,$$
$$h_2 \equiv E^2 * R^2 + 2 * E * R * (R - b) - a^2 = 0.$$

注意到显然有 $r_0 \leq 2R$, 于是，当 C_0 沿正 y 轴移动时应该有最大值，其中, $-\infty < b < 0$ 或 $0 < b < +\infty$ 且 $a < R < +\infty$. 为了在约束条件 $h_1 = 0$, $h_2 = 0$ 下，决定在由上述不等式表明的 b, R 的开域内 E 的极值. 如 §5.5 一样，我们引入 Lagrange 乘子 λ_1, λ_2 和 Lagrange 多项式

$$L \equiv E + \lambda_1 * h_1 + \lambda_2 * h_2.$$

容易发现对于 Lagrange 多项式集 LAG 和 Jacobi 多项式集 JAC 我们有 $\mathrm{Zero}_{\mathbf{R}}(JAC) = \emptyset$, 而 $\mathrm{Zero}_{\mathbf{R}}(LAG)$ 只含有一个极值 $\frac{1}{2}$, 它对应于 $b = \frac{1}{\sqrt{3}}, R = \frac{2}{\sqrt{3}}$. 这就说明了当 AB 固定时，如果三角形 ABC 等边时，E 取最大值 $\frac{1}{2}$. 由于,

极值 $\frac{1}{2}$ 与边 AB, 或者说 $a \neq 0$, 无关, 所以同样的结论对于边 AB 变动时也成立. □

注意到用同样的方法可以证明当 r 为边 AB 的外切圆的半径时, Euler 比例的极值将不存在.

第八章　在其他方面的应用

§8.1　在自动发现未知关系和自动确定几何轨迹方面的应用

记号 $\mathbf{K}, X = (x_1, \cdots, x_n)$ 等如前所述.

未知关系的自动发现

考虑一个三条边已知的三角形. 这个三角形除可以在平面上作刚体运动外可以完全确定. 特别地，这个三角形的面积可以完全确定. 该面积必然由三条边组成的某个表达式确定. 而且，如果考虑三角形的方向，那么根据已知边，面积将为两个符号相反的值. 所以，猜想一个三角形的面积的平方是三条边的某个 *有理* 表达式是合理的. 现在的问题是如何确定由以上分析推知应存在的表达式的 *精确* 形式. 当然，这种精确的表达式在数学史上很早有了，古欧洲的 Heron 公式和中国古代的秦氏公式，参见第二章例 2.1.2 和公式 (2.3.20).

秦氏公式和 Heron 公式确实彼此等价，但是它们的推导是十分的巧思并且更十分的复杂. 于是是否存在一个较为简单且自然的方法，用此方法也可以得到这些公式的问题便出现了. 因为有许多类似的、确定假定存在或是已知存在的未知关系的问题，所以我们将此类问题归纳成以下一般性问题:

问题 UR　发现某些几何 (或代数) 对象间可能存在的未知关系.

最简单的例子之一是假定三角形面积和三条边的关系未知，发现这一关系. 为了解决问题 UR 我们采用以下一般方法和基本的原理.

原理和方法　令 HYP 为多项式集，它的零点表示该问题的基本几何条件. 变量 x_i 将按下述方式选择并排列: 前几个 x_i 恰好是所求关系中的几何 (或代数) 实体. 令 CS 为 HYP 的特征列, C_i 为 CS 中的多项式. 根据整序原理，我们有

$$\mathrm{Zero}(HYP) \subset \mathrm{Zero}(CS). \tag{8.1.1}$$

因此，我们总能得到 $C_1 = 0$, 而这通常恰为我们所寻求的关系.

关于距离、面积和体积的例子

例 8.1.1 (关于三角形面积的秦 -Heron 公式)　令 x_1, x_2, x_3, x_4 分别表示三角形 $A_0A_1A_2$ 的三条边 $|A_0A_1|, |A_0A_2|, |A_1A_2|$ 和三角形的面积，我们要求它们

之间假定未知的关系. 选定坐标, 使得

$$A_0 = (0,0),\ A_1 = (x_5,0),\ A_2 = (x_6,x_7).$$

注意 A_0, A_1, A_2 坐标中的变量 x_i 按如下方式选择: 按自然序与 $x_1,\cdots,x_4$ 相接. 几何条件可化为方程组 $HYP=0$, 其中 $HYP=\{h_1,h_2,h_3,h_4\}$ 且

$$\left.\begin{aligned} h_1 &= 2*x_4 - x_5*x_7,\\ h_2 &= x_5 - x_1,\\ h_3 &= x_2^2 - x_6^2 - x_7^2,\\ h_4 &= x_3^2 - (x_6-x_5)^2 - x_7^2. \end{aligned}\right\} \tag{8.1.2}$$

易发现它的特征列由 4 个多项式组成, 其中第一个多项式为

$$C_1 = 2*x_1^2*x_2^2 + 2*x_1^2*x_3^2 + 2*x_2^2*x_3^2 - x_1^4 - x_2^4 - x_3^4 + 16*x_4^2. \tag{8.1.3}$$

关系式 $C_1 = 0$ 恰为所求的秦 -Heron 公式.

例 8.1.2 (四面体的体积与边的关系) 令四面体 $A_0A_1A_2A_3$ 的体积为 x_7, 六条边为

$$\begin{aligned} &|A_0A_1| = x_1,\ |A_0A_2| = x_2,\ |A_0A_3| = x_3,\\ &|A_1A_2| = x_4,\ |A_1A_3| = x_5,\ |A_2A_3| = x_6. \end{aligned} \tag{8.1.4}$$

指定四个顶点的坐标为 $x_i(i>7)$, 使得

$$A_0 = (0,0,0),\ A_1 = (x_8,0,0),\ A_2 = (x_9,x_{10},0),\ A_3 = (x_{11},x_{12},x_{13}). \tag{8.1.5}$$

于是, 我们得到一个多项式方程组 $h_i = 0,\ i = 1,\cdots,7$, 该多项式方程组用变量 $x_1,\cdots,x_{13}$ 给出了四面体的体积和边, 其中 h_i 给出如下:

$$\left.\begin{aligned} &h_1 = 6*x_7 + x_8*x_{10}*x_{13},\\ &h_2 = x_8 + x_1,\\ &h_3 = x_2^2 - x_9^2 - x_{10}^2,\\ &h_4 = x_3^2 - x_{11}^2 - x_{12}^2 - x_{13}^2,\\ &h_5 = x_4^2 - (x_9-x_8)^2 - x_{10}^2,\\ &h_6 = x_5^2 - (x_{11}-x_8)^2 - x_{12}^2 - x_{13}^2,\\ &h_7 = x_6^2 - (x_{11}-x_9)^2 - (x_{10}-x_{13})^2. \end{aligned}\right\} \tag{8.1.6}$$

现在求多项式集 $HYP = \{h_1, \cdots, h_7\}$ 的特征列 CS, 易发现对于第一个特征多项式 C_1, 方程 $C_1 = 0$ 将自动给出用 $x_1, \cdots, x_6$ 表示的体积 x_7 的表达式:

$$144 * x_7^2 = -\sum_1 (x_1^2 * x_6^4 + x_6^2 * x_1^4) + \sum_2 (x_2^2 * x_1^2 * x_5^2) - \sum_3 (x_1^2 * x_2^2 * x_4^2). \tag{8.1.7}$$

公式中的和号 $\sum_i$ 表示在以下指定的各自的范围中展开:

$\sum_1$ 是关于 3 组反向边 $(x_1, x_6), (x_2, x_5), (x_3, x_4)$ 求和;

$\sum_2$ 是关于 12 个非闭合边的三元组 (x_2, x_1, x_5) 求和;

$\sum_3$ 是关于 4 个能够形成像 (x_1, x_2, x_4) 一样的的三角形的边的三元组求和.

考虑一个特殊的情况, 即四面体退化为一个平面图的情形, 四面体的体积为 0, 则方程 (8.1.7) 就变成

$$-\sum_1 + \sum_2 - \sum_3 = 0, \tag{8.1.8}$$

上式给出了位于同一平面的四点间六个相互距离的关系. 注意方程 (8.1.8) 关于 6 条边 $x_i (i = 1, \cdots, 6)$ 是齐次的, 且每条边的次数为 4, 直接从几何的角度来考虑这是显然的.

注释 8.1.3 我们可以提出像例 8.1.1 和 8.1.2 的问题, 即关于 4 维欧氏空间 $\mathbf{R}^4$ 中的 4- 单形的体积和 5 维空间 $\mathbf{R}^5$ 中的 5- 单形的体积, 以及 $\mathbf{R}^3$ 中的 5 点的相互距离间关系, 或是 $\mathbf{R}^4$ 中 6 点的相互距离间的关系. 我们甚至可以在一个维数任意但 *固定* 的欧氏空间中提出同样的问题. 只要事先固定欧氏空间的维数, 内存空间足够, 并且计算机的运行时间允许我们做这样的计算, 就能用以上同样的方法解决这些问题. 另一方面, 对于一般维数 n, 这样一个公式的确定完全是我们的机械化方法所不能做到的. 注意 Cayley 等已经通过对行列式进行巧妙处理而发现了这些公式. 这表明虽然计算机在数学研究方面给我们提供了强有力的工具, 但我们并不能仅仅依赖计算机, 而不求助于通常的数学方法.

Gauss *五边形定理*

例 8.1.4 (Gauss 五边形定理) 在 [Gau2] 中的一段简短的备注中, C. F. Gauss 解决了一个有趣的问题, 问题如下:

任意给定一个五边形 $ABCDE$, 欲求出五个三角形 EAB, ABC, BCD, CDE, DEA 的面积和原五边形 $ABCDE$ 的面积的关系.

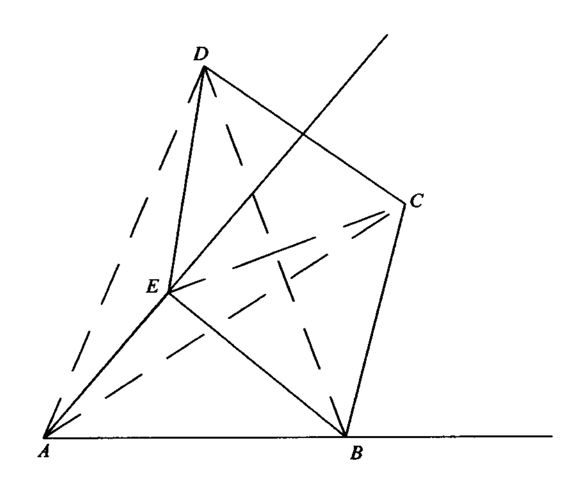


图 8.1 Gauss 五边形定理

高斯采用一种巧妙的方法解决了这个问题. 他似乎假定五边形 $ABCDE$ 是凸的. 采用我们的一般方法, 我们解决了该问题, 如下所示.

假定 A, B, E 不共线, 令 AB, AE 为坐标系的 X 轴和 Y 轴. 依据我们的基本原理, 将 5 个三角形 ABC, BCD, CDE, DEA, EAB 的面积和五边形 $ABCDE$ 的面积分别记为 $x_1, \cdots, x_6$. 注意所有的面积都依照所指定的顶点的顺序视为有向. 不论五边形是否为凸的, 我们都有

$$\text{面积}(ABCDE) = \text{面积}(ABC) + \text{面积}(ACD) + \text{面积}(ADE).$$

现在令顶点坐标为

$$A = (0,0),\ B = (x_7, 0),\ C = (x_8, x_9),\ D = (x_{10}, x_{11}),\ E = (0, x_{12}).$$

注意在斜角坐标中, 当顶点的序为 $(x_i, y_i), (x_j, y_j), (x_k, y_k)$ 时, 三角形的有向面积为

$$\frac{1}{2} * \begin{vmatrix} x_i & y_i & 1 \\ x_j & y_j & 1 \\ x_k & y_k & 1 \end{vmatrix},$$

至多相差一些仅依赖于坐标系统的非零定值 D. 于是, 这样我们得到假设多项式集 $HYP = \{h_1, \cdots, h_6\}$, 其中 h_i 如下所示, 非零定值 D 已去掉:

$$\left.\begin{aligned}
&h_1 = 2 * x_1 - x_7 * x_9,\\
&h_2 = 2 * x_2 - x_7 * x_9 - x_8 * x_{11} + x_9 * x_{10} + x_7 * x_{11},\\
&h_3 = 2 * x_3 - x_8 * x_{11} - x_{10} * x_{12} + x_8 * x_{12} + x_9 * x_{10},\\
&h_4 = 2 * x_4 - x_{10} * x_{12},\\
&h_5 = 2 * x_5 - x_7 * x_{12},\\
&h_6 = 2 * x_6 - 2 * x_1 - x_8 * x_{11} + x_9 * x_{10} - 2 * x_4.
\end{aligned}\right\} \tag{8.1.9}$$

HYP 的特征列为 $CS = \{C_1, \cdots, C_6\}$, 其中第一个特征多项式 C_1 为

$$\begin{aligned}
C_1 \;=\; & x_6^2 - (x_1 + x_2 + x_3 + x_4 + x_5) * x_6\\
& + (x_1 * x_2 + x_2 * x_3 + x_3 * x_4 + x_4 * x_5 + x_5 * x_1).
\end{aligned} \tag{8.1.10}$$

关系式 $C_1 = 0$ 恰为高斯所给的漂亮的公式. 注意这里并不需要预先假定五边形为凸的. 但为了选择坐标轴, 要求点 A, B, E 不共线, 否则, 就是完全任意的. 如果需要的话, 我们可以将点 A, B, E 共线的条件加入条件集, 以观察在这种退化条件下会发生什么. 但这没有什么几何意义, 因此我们就可以满意地讨论到这里.

更多的几何例子

例 8.1.5 用一个四面体的 6 条边来确定该四面体的外接球 S 的外半径. 取坐标使得四面体的 4 个顶点和 6 条边像 (8.1.4) 和 (8.1.5) 中所给出的一样. 令外接球 S 的外心为 (x_{14}, x_{15}, x_{16}), 外半径为 x_7'. 对于假设我们得到由 (8.1.6) 中的多项式 $h_2, \cdots, h_7$ 和下列多项式 h_1', h_8, h_9, h_{10} 组成的多项式集 HYP':

$$\left.\begin{aligned}
&h_1' = x_7'^2 - x_{14}^2 - x_{15}^2 - x_{16}^2,\\
&h_8 = x_7'^2 - (x_{14} - x_8)^2 - x_{15}^2 - x_{16}^2,\\
&h_9 = x_7'^2 - (x_{14} - x_9)^2 - (x_{15} - x_{10})^2 - x_{16}^2,\\
&h_{10} = x_7'^2 - (x_{14} - x_{11})^2 - (x_{15} - x_{12})^2 - (x_{16} - x_{13})^2.
\end{aligned}\right\} \tag{8.1.11}$$

HYP' 的特征列 CS' 中的第一个多项式 C_1' 很容易确定. 将 8.1.2 中的特征多项式 C_1 与和 $\sum_i$ 进行比较, 易发现以下公式:

$$9 * \mathrm{Vol}^2 * \mathrm{Diam}^2 = \sigma * (\sigma - \alpha) * (\sigma - \beta) * (\sigma - \gamma), \tag{8.1.12}$$

其中 Vol, Diam 分别表示四面体的体积和外接球 S 的直径, 而

$$\sigma = \frac{\alpha + \beta + \gamma}{2}, \tag{8.1.13}$$

$$\alpha = x_1 * x_6,\ \beta = x_2 * x_5,\ \gamma = x_3 * x_4 \tag{8.1.14}$$

分别对应于三组反向边 x_1, x_6; x_2, x_5; x_3, x_4.

注释 8.1.6 作者并不知道在过去文献的何处可以找到公式 (8.1.12), 这里通过自动推理的方法得到公式 (8.1.12), 注意 Vol = 0 时四点共圆 Ptolemy 公式与 (8.1.12) 右侧的联系.

<u>双曲平面的距离和面积</u>

我们的方法适用于任一种几何. 为说明这一点, 考虑平面双曲几何, 后面将会用 Beltrami 坐标. 我们注意到在非欧几何的研究中, 超越函数被频繁使用. 另一方面, 我们的方法只能处理纯代数特征的多项式. 但是, 因为我们处理超越函数间的代数关系而不是超越函数本身, 所以对于我们的方法的应用来说这并不是一个难以逾越的障碍. 确实在书 [WWT5] 和早期关于机器定理证明的论文 [WWT1] 中, 已经有一些例子说明如何处理这些包括超越函数在内的问题, 下例再次说明了实现的方法.

例 8.1.7 发现双曲平面上 4 点间 6 个距离之间的关系.

对 4 个给定的点 A_0, A_1, A_2, A_3 间的 6 个距离 A_iA_j, 令

$$\left.\begin{array}{l} x_1 = \cosh A_0A_1,\ x_2 = \cosh A_0A_2,\ x_3 = \cosh A_0A_3, \\ x_4 = \cosh A_1A_2,\ x_5 = \cosh A_1A_3,\ x_6 = \cosh A_2A_3. \end{array}\right\} \tag{8.1.15}$$

现在取定坐标系, 且取 4 个点 A_i 的 Beltrami 坐标, 如下所示:

$$A_0 = (0,0),\ A_1 = (x_7, 0),\ A_2 = (x_8, x_9),\ A_3 = (x_{10}, x_{11}).$$

我们得到假设多项式集 $HYP = \{h_1, \cdots, h_6\}$, 如下给出:

$$\left.\begin{array}{rl} h_1 = & x_1^2 - x_1^2 * x_7^2 - 1, \\ h_2 = & x_2^2 - x_2^2 * x_8^2 - x_2^2 * x_9^2 - 1, \\ h_3 = & x_3^2 - x_3^2 * x_{10}^2 - x_3^2 * x_{11}^2 - 1, \\ h_4 = & x_4 - x_1 * x_2 + x_1 * x_2 * x_7 * x_8, \\ h_5 = & x_5 - x_1 * x_3 + x_1 * x_3 * x_7 * x_{10}, \\ h_6 = & x_6 - x_2 * x_3 + x_2 * x_3 * x_8 * x_{10} + x_2 * x_3 * x_9 * x_{11}. \end{array}\right\} \tag{8.1.16}$$

HYP 的特征列的第一个多项式 C_1 由下式给出:

$$C_1 = (x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2) - (x_1^2 * x_6^2 + x_2^2 * x_5^2 + x_3^2 * x_4^2)$$

$$
\begin{aligned}
&- 2*(x_1*x_3*x_5+x_1*x_2*x_4+x_2*x_3*x_6+x_4*x_5*x_6)\\
&+ 2*(x_1*x_4*x_3*x_6+x_1*x_2*x_5*x_6+x_2*x_4*x_3*x_5)\\
&- 1.
\end{aligned} \tag{8.1.17}
$$

方程 $C_1 = 0$ 即为所求的关系.

例 8.1.8　在双曲平面中用三角形的 3 条边确定三角形的面积 $\triangle$.

对三角形 $A_0A_1A_2$ 的边和面积 $\triangle$, 令

$$
\left.\begin{aligned}
x_1 = \cosh\ A_0A_1,\quad x_2 = \cosh\ A_0A_2,\ x_3 = \cosh\ A_1A_2,\\
x_4 = \cos\ \triangle,
\end{aligned}\right\} \tag{8.1.18}
$$

则有

$$
\pi - \triangle = \alpha_0 + \alpha_1 + \alpha_2, \tag{8.1.19}
$$

其中 $\alpha_0, \alpha_1, \alpha_2$ 为三角形的三个内角. 取坐标系使得

$$
A_0 = (0,0),\ A_1 = (x_5, 0),\ A_2 = (x_6, x_7).
$$

令

$$
\left.\begin{aligned}
x_{10} = \cos\ \alpha_0,\quad x_{11} = \sin\ \alpha_0,\\
x_{12} = \cos\ \alpha_1,\quad x_{13} = \sin\ \alpha_1,\\
x_{14} = \cos\ \alpha_2,\quad x_{15} = \sin\ \alpha_2.
\end{aligned}\right\} \tag{8.1.20}
$$

由此得到假设多项式集 $HYP = \{h_1, \cdots, h_{12}\}$, 其中 h_i 如下:

$$
\left.\begin{aligned}
h_1 &= x_1^2 - x_1^2 * x_5^2 - 1,\\
h_2 &= x_2^2 - x_2^2 * x_6^2 - x_2^2 * x_7^2 - 1,\\
h_3 &= x_3 - x_1 * x_2 + x_1 * x_2 * x_5 * x_6,\\
h_4 &= x_8^2 - x_6^2 - x_7^2,\\
h_5 &= x_9^2 - x_7^2 - x_1^2 * (x_5 - x_6)^2,\\
h_6 &= x_8 * x_{10} - x_6,\\
h_7 &= x_9 * x_{12} - x_1 * (x_5 - x_6),\\
h_8 &= x_8 * x_{11} - x_7,\\
h_9 &= x_9 * x_{13} - x_7,\\
h_{10} &= x_8 * x_9 * x_{14} - x_1 * x_7^2 + x_1 * x_6 * (x_5 - x_6),\\
h_{11} &= x_2 * x_8 * x_{15} - x_1 * x_5 * x_{13},\\
h_{12} &= x_{10} * x_{13} * x_{15} + x_{11} * x_{12} * x_{15} + x_{11} * x_{13} * x_{14}\\
&\quad - x_{10} * x_{12} * x_{14} - x_4.
\end{aligned}\right\} \tag{8.1.21}
$$

对于第一个特征多项式 C_1, 方程 $C_1 = 0$ 可写成以下形式:

$$(x_1+1)*(x_2+1)*(x_3+1)*(x_4-1)$$
$$= x_1^2+x_2^2+x_3^2-2*x_1*x_2*x_3-1. \qquad (8.1.22)$$

分别用边的双曲余弦和面积的双曲余弦替换 x_i, $i=1,\cdots,4$, 我们看到最后一个方程与 [Gr] 中 361 页的例 27 所给的形式等价, 该方程在这里用自动的方法得到了.

注释 8.1.9 近年来在双曲空间中用一个四面体的六条边确定该四面体的体积在文献中讨论得很深入. 但是, 如 Dehn(例如参见 [Kl], p.203) 所指出的一样, 与三角形在双曲空间中的情形不同, 这样一个四面体的体积并不能用该四面体各边间的二面角来表示. 而且, 以前也早已证明, 双曲四面体的表达式包含高阶的超越函数, 即所谓的 Lobachevsky 函数. 所以是否可以用例 8.1.8 所用方法, 即用 6 条边来确定一个四面体的体积, 尚不能确定. 这作为一个问题留待以后研究.

<u>未知代数关系的自动确定</u>

我们的一般原理和方法不仅可以应用于几何问题, 而且可以应用于代数问题. 以下是一个用以说明的最简单的示例之一.

例 8.1.10 (Newton 公式) 用 n 次代数方程的系数确定该方程根的 k 阶幂次的和.

正如注释 8.1.3 所述, 对每一对 *固定* 的整数 k,n, 但绝不是 *一般的* 整数对, 基本上可以自动确定这样的表达式. 为说明这一点, 取 $k=4, n=4$. 依照一般原理, 将代数方程 E_4 写为关于单变元 z 的次数 $n=4$ 的形式:

$$E_4\colon\ z^4+x_1*z^3+x_2*z^2+x_3*z+x_4=0. \qquad (8.1.23)$$

令 x_5,x_6,x_7,x_8 为根的 k 阶幂次和, 其中 $k=1,2,3,4$. 问题变为通过消去 x_8, 得到关于 x_7,x_6,x_5 和 x_1,x_2,x_3,x_4 的递推关系式. 为此, 令方程 E_4 的四个根为 x_9,x_{10},x_{11},x_{12}. 又假设多项式集 $HYP=\{h_1,\cdots,h_7\}$, 其中 h_i 如下所示:

$$\left.\begin{aligned}
h_1 &= x_9+x_{10}+x_{11}+x_{12}+x_1,\\
h_2 &= x_9*x_{10}+x_9*x_{11}+x_9*x_{12}\\
&\qquad +x_{10}*x_{11}+x_{10}*x_{12}+x_{11}*x_{12}-x_2,\\
h_3 &= x_9*x_{10}*x_{11}+x_9*x_{10}*x_{12}+x_{10}*x_{11}*x_{12}+x_3,\\
h_4 &= x_9*x_{10}*x_{11}*x_{12}-x_3,\\
h_5 &= x_6-(x_9^2+x_{10}^2+x_{11}^2+x_{12}^2),\\
h_6 &= x_7-(x_9^3+x_{10}^3+x_{11}^3+x_{12}^3),\\
h_7 &= x_8-(x_9^4+x_{10}^4+x_{11}^4+x_{12}^4).
\end{aligned}\right\} \qquad (8.1.24)$$

对于 HYP 的特征集 CS, 我们看到前三个特征多项式为

$$\begin{aligned}
C_1 &= x_6 + 2 * x_2 - x_1^2, \\
C_2 &= x_7 + 3 * x_3 - 3 * x_2 * x_1 + x_1^3, \\
C_3 &= x_8 + 4 * x_4 - 4 * x_3 * x_1 - 2 * x_2^2 + 4 * x_2 * x_1^2 - x_1^4.
\end{aligned} \tag{8.1.25}$$

方程 $C_i = 0$, $i = 1, 2, 3$, 即为所求的 $k = 2, 3, 4$, $n = 4$ 时的牛顿公式.

高小山在他的博士论文 [Gao1](亦可参考文献 [WWD]) 中对一个有趣的问题进行了详细的研究. 参看以下的例子.

例 8.1.11 (判别式系统) 假设给定一个关于单变元 z 的次数为 n 的代数方程 E_n 以及 n 的一个分划 $\Pi = (\pi_1, \cdots, \pi_k)$. 确定方程 E_n 的系数所应满足的条件, 使得 E_n 的根如已给出的分划 Π 一样被划分.

假设次数 $n = 4$, 固定分划 $\Pi = (2, 2)$. 将方程 E_4 写成 (8.1.23) 的形式. 令 4 个根为 x_5, x_5, x_6, x_6. 即得假设集 $HYP = \{h_1, h_2, h_3, h_4\}$, 其中 h_i 给出如下:

$$\left.\begin{aligned}
h_1 &= 2 * (x_5 + x_6) + x_1, \\
h_2 &= (x_5^2 + 4 * x_5 * x_6 + x_6^2) - x_2, \\
h_3 &= 2 * x_5 * x_6 * (x_5 + x_6) + x_3, \\
h_4 &= x_5^2 * x_6^2 - x_4.
\end{aligned}\right\} \tag{8.1.26}$$

HYP 的特征列的前两个多项式 C_1, C_2 给出了所求的条件:

$$\left.\begin{aligned}
C_1 &\equiv 8 * x_3 - 4 * x_2 * x_1 + x_1^3 = 0, \\
C_2 &\equiv 54 * x_4 - 16 * x_2^2 + 8 * x_2 * x_1^2 - x_1^4 = 0.
\end{aligned}\right\} \tag{8.1.27}$$

注意我们并没有排除 $x_5 = x_6$ 的可能性, 故该条件应包括分划 (2, 2) 和 (4).

注释 8.1.12 最近, 杨路将上述判别式系统扩展到考虑根的存在性的情况, 参见 [Y-H-Z] 和 [Y-Z-H].

几何定理的自动发现

我们的一般性方法也给我们提供了一种自动发现几何定理, 甚至是新定理的方法. 以下是一个简单的示例.

例 8.1.13 重新考虑例 (7.2.5) 中的 Feuerbach 定理. 假定我们对于三角形的九点圆和内切圆或者旁切圆之间的任何可能存在的关系一无所知. 为了发现其中任一个可能的关系, 令两圆的半径分别为 x_2 和 x_1, 两圆中心的距离为 x_3,

取坐标使

$$I=(0,x_1),\ A=(x_4,0),\ B=(x_5,0),\ C=(x_6,x_7),\ N=(x_8,x_9).$$

于是多项式集变为 $HYP'=\{h'_1,\cdots,h'_6\}$, 其中 h_i 如下所示:

$$\left.\begin{aligned}
h'_1 &= (x_1^2+x_4*x_5)*x_6 - x_1^2*(x_4+x_5),\\
h'_2 &= (x_1^2+x_4*x_5)*x_7 - 2*x_1*x_4*x_5,\\
h'_3 &= 4*x_8 - (x_4+x_5+2*x_6),\\
h'_4 &= 4*x_7*x_9 - x_7^2 - (x_5-x_6)*(4*x_8-2*x_4-x_5-x_6),\\
h'_5 &= 4*x_2^2 - (2*x_8-x_4-x_5)^2 - 4*x_9^2,\\
h'_6 &= x_3^2 - x_8^2 - (x_9-x_1)^2.
\end{aligned}\right\} \tag{8.1.28}$$

结果, 对于 $x_1*x_2*x_7*x_9\neq 0$, wsolve 给出 HYP' 的 4 个特征集 CS_i, $i=1,2,3,4$, 其中第一个特征多项式 C_{i1} 如下:

$$\left.\begin{aligned}
C_{11}=-x_3+x_2+x_1,\ C_{21}=x_3-x_2+x_1,\\
C_{31}=-x_3-x_2+x_1,\ C_{41}=x_3+x_2+x_1.
\end{aligned}\right\} \tag{8.1.29}$$

关系式 $C_{i1}=0$ 表明九点圆和内切圆或旁切圆按某种相切的方式相切. 依据一般性理论, 我们有

$$\mathrm{Zero}(HYP'/x_1*x_2*x_7*x_9)\subset\bigcup_i \mathrm{Zero}(CS_i)\subset\bigcup_i \mathrm{Zero}(C_{i1}).$$

这样我们用自动的方法也发现了 Feuerbach 定理.

几何轨迹的自动推导

某种几何条件下一个动点的轨迹的确定恰为确定在该条件下该点的坐标间的关系. 我们得到自动确定未知关系的一般性方法可以应用到当前这种情形. 考虑以下问题.

定义 8.1.14 4- 连杆 是一个三条杆 AU,UV,VB 组成的机构, 这三条杆在轴 U,V 处联接, 杆的末端 A,B 固定, 杆 AU,BV 分别绕定点 A,B 转动.

包含该连杆的平面称为 连结平面.

杆 UV 称为 连结杆.

标注在对偶杆 UV 的移动平面上的某定点称为 连结点.

杆 AU,BV 绕 A,B 转动时对偶点 Z 的轨迹称为 连结曲线.

例 8.1.15 (连结曲线)　确定连结点 Z 的几何轨迹，即连结曲线.

为了简化计算，用复数表示连杆平面中的点．这样，对每个点 P 可以用相应的复数和共轭复数 P_1, P_2 来表示．令杆 UV 所在的斜面的方向为从 U 指向 V, 与实轴的夹角为 θ. 有向角 $\angle(UV,UZ), \angle(UV,VZ)$, UZ, VZ 的边长分别记为 α,β,s_b,s_a. 令 ($\sqrt{-1}=\mathbf{i}$)

$$\left.\begin{array}{l} e^{\mathbf{i}*\theta}=\tau_1,\quad s_b*e^{\mathbf{i}*\alpha}=\mu_1,\quad s_a*e^{\mathbf{i}*\beta}=\nu_1, \\ e^{-\mathbf{i}*\theta}=\tau_2,\ s_b*e^{-\mathbf{i}*\alpha}=\mu_2,\ s_a*e^{-\mathbf{i}*\beta}=\nu_2. \end{array}\right\} \tag{8.1.30}$$

如果通过点 Z 作一条 UV 的垂线 ZW, 垂足为 W, 则有

$$\begin{array}{l} \mathrm{Im}(\mu_1)=\mathrm{Im}(\mu_2)=\mathbf{i}*h, \\ \mathrm{Re}(\mu_1)=s,\ \mathrm{Re}(\nu_1)=s-r, \end{array} \tag{8.1.31}$$

其中 Re, Im 分别表示实部和虚部，将有向线段 UV 上的有向长度 UW, VW 分别记为 $s, s-r$, 参见图 8.2.

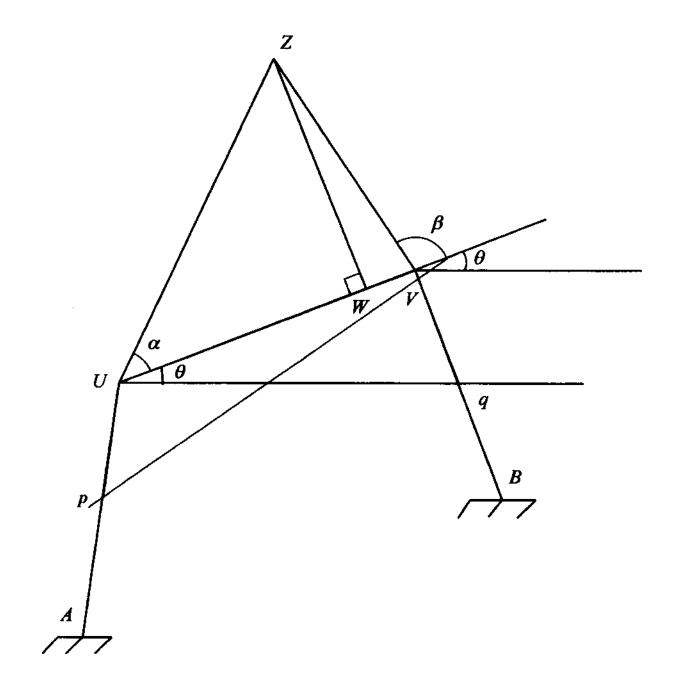


图 8.2　4- 连杆

令杆 AU, BV, UV 的绝对长度分别为 p, q 和 r. 我们需要用可以转化为 9 个实值参数的已知值 $A_1, A_2, B_1, B_2, p, q, r, h, s$, 确定点 Z 的轨迹或是共轭复数

Z_1, Z_2 满足的方程. 有假设多项式集 $HS = \{h_1, \cdots, h_6\}$, 其中

$$\left.\begin{aligned} h_1 &= (U_1 - A_1) * (U_2 - A_2) - p^2, \\ h_2 &= (V_1 - B_1) * (V_2 - B_2) - q^2, \\ h_3 &= U_1 + \tau_1 * \mu_1 - Z_1, \\ h_4 &= U_2 + \tau_1 * \mu_1 - Z_2, \\ h_5 &= V_1 + \tau_1 * \nu_1 - Z_1, \\ h_6 &= V_2 + \tau_1 * \nu_1 - Z_2, \end{aligned}\right\} \tag{8.1.32}$$

将变量按下序排列

$$\begin{aligned} p \quad &\prec q \prec r \prec A_1 \prec A_2 \prec B_1 \prec B_2 \prec \mu_1 \prec \mu_2 \prec \nu_1 \prec \nu_2 \\ &\prec Z_1 \prec Z_2 \prec U_1 \prec U_2 \prec V_1 \prec V_2 \prec \tau_1 \prec \tau_2, \end{aligned}$$

则特征列的第一个特征多项式 C_1 按以下形式给出轨迹方程:

$$C_1 \equiv Z_1^3 * Z_2^3 * (\mu_1 - \nu_1) * (\mu_2 - \nu_2) + \cdots = 0. \tag{8.1.33}$$

方程 $C_1 = 0$ 用已知参数来表示 Z_1, Z_2, 项数为 362 项. 如果我们用实坐标

$$Z = (x, y), \ A = (a_x, a_y), \ B = (b_x, b_y),$$

和实参数 p, q, r, h, s 表示方程, 则 C_1 将有 2016 项, 每个运行坐标 x, y 是次数为 6, 最高项为 $(x^6 + y^6) * r^2$.

注释 8.1.16 以上几何轨迹, 作为平面上的点集, 实际上只是 $\mathrm{Proj}\,\mathrm{Zero}(HS) \subset \mathrm{Zero}(C_1)$ 中的一部分, 其中 Proj 是从 Z_1, Z_2 等空间到 $\mathbf{R}^2(x, y)$ 上的自然投影. 用第 5 章第 4 节中所述的基于射影定理的方法可以完全确定轨迹, 但该方法可能过于复杂以致于不能被接受. 目前的方法虽然并不十分完备甚至于不精确, 但用于求解该问题却是相当合理的捷径. 实际上, 这正是实践和文献中广泛采用的方法.

§8.2 在不等式、优化问题和非线性规划等问题方面的应用

令 $\mathbf{R}$ 为实数域, $X = (x_1, \cdots, x_n)$ 等如前所述.

<u>含有不等式的问题</u>

或许 Collins 的 CAD 方法 (参见文献 [Col1], [Ar1]) 是用于解决含有不等式问题的最为通用和完备的方法. 另一方面, 在 §5.5 中, 我们展示过定理 5.5.37

和定理 5.5.38 中的方法. 尽管它并不像 Collins 的方法那样通用完备, 但对于某一类问题效率似乎更高. 除了在 §7.3 中已经考虑过的含有不等式的几何定理的证明外, 应用范围还包括了不等式的证明、代数或几何、非线性规划以及优化问题等等. 我们对所有这类问题都感兴趣, 它们可以简化为以下形式:

问题 Ineq 令 $\mathbf{R}^n(X)$ 为 n 维实欧氏空间坐标 $X=(x_1,\cdots,x_n)$, D 为 E^n 中的区域. 令 f,h_i $(i\in I=\{1,\cdots,r\},r<n)$, 及 g 为 $\mathbf{R}^n[X]$ 中区域 D 上的实多项式, 确定实值 c 取何值时总有

$$f\geq c \text{ 或 } f>c \text{ 或} f\leq c \text{ 或 } f<c \tag{8.2.34}$$

且满足条件

$$HS=0, \text{ 其中 } HS=\{h_i \mid i\in I\}, \tag{8.2.35}$$

和

$$g\neq 0. \tag{8.2.36}$$

为了方便读者, 我们将用于确定不等式问题的最 (最大或最小) 优值 (假定存在) 的定理 5.5.37 和 5.5.38 基本公式在下面重写一遍. (D 为开域或闭域, O 为开域):

$$\text{Optm }\{f,D,HS\}=\text{Optm Ker}\{f,D,HS\}. \tag{$*$}$$

其中

$$\left.\begin{aligned}&\text{Optm }\{f,g,O,HS\}=\text{Optm}_{X\in O}\ \{f(X)\mid X\in LJVal\},\\&LJVal=\text{LProj }\tilde{O}\text{Zero}_{\mathbf{R}}(LS/g)+O\text{Zero}_{\mathbf{R}}(JS/g).\end{aligned}\right\} \tag{$**$}$$

在 (**) 中, LS 和 JS 分别表示相关问题的 Lagrange 多项式集和 Jacobi 多项式集.

<u>确定多项式的正定性</u>

在最简单的应用中, 我们可以引用关于确定多项式是否正定或半正定的研究, 在这方面可以参见作者的相关文献和王东明的文章 [WDM5].

例 8.2.1 (Motztkin 多项式) Motztkin 多项式 M 为

$$M=1+x_1^2*x_2^4+x_1^4*x_2^2-3*x_1^2*x_2^2, \tag{8.2.37}$$

在整个平面 $\mathbf{R}^2(x_1,x_2)$ 上是半正定的.

证明 首先，从简单次数考虑，可知平面上必存在 M 的最小值. 现引入新的变量 x_0, 并令

$$h_0 = M - x_0. \tag{8.2.38}$$

问题简化为证明满足约束条件 $h_0 = 0$ 的 x_0 的最小值 ≥ 0. 有两种方法可以用于确定最小值.

第一种方法基于定理 5.5.38, 用 Lagrange 乘子 λ 生成 Lagrange 多项式.

$$L = x_0 + \lambda * (M - x_0). \tag{8.2.39}$$

Lagrange 多项式集为

$$\begin{aligned} LS &= \left\{\frac{\partial L}{\partial x_k}, h_0 \mid k = 0,1,2\right\} \\ &= \{1 - \lambda,\ 2 * x_1 * x_2^2 * \lambda * (x_2^2 + 2 * x_1^2 - 3), \\ &\quad 2 * x_1^2 * x_2 * \lambda * (2 * x_2^2 + x_1^2 - 3),\ M - x_0\}. \end{aligned} \tag{8.2.40}$$

易知

$$\mathrm{Zero}_{\mathbf{R}}(LS) = \bigcup_{k=1,2,3} \mathrm{Zero}_{\mathbf{R}}(CS_k), \tag{8.2.41}$$

其中

$$\left.\begin{aligned} CS_1 &= \{x_0 - 1, x_1, \lambda - 1\}, \\ CS_2 &= \{x_0 - 1, x_2, \lambda - 1\}, \\ CS_3 &= \{x_0, x_1^2 - 1, x_2^2 - 1, \lambda - 1\}. \end{aligned}\right\} \tag{8.2.42}$$

把 $\mathbf{R}^3(x_0, x_1, x_2)$ 到 $\mathbf{R}(x_0)$ 的投影记为 Proj_0, 则有

$$\mathrm{Proj}_0\ \mathrm{Zero}_{\mathbf{R}}(LS) = \{0, 1\}. \tag{8.2.43}$$

另一方面，对于 Jacobi 多项式集

$$JS = \left\{\frac{\partial h_0}{\partial x_k},\ h_0 \mid k = 0,1,2\right\}, \tag{8.2.44}$$

显然有

$$\mathrm{Zero}_{\mathbf{R}}(JS) = \emptyset. \tag{8.2.45}$$

根据定理 5.5.38, 可得

$$\mathrm{Least}\{x_0, \mathbf{R}^3, h_0\} = \mathrm{Least}\{0,1\} = 0 \tag{8.2.46}$$

或 $M \geq 0$, 如欲所证. 而且, 从 CS_3 可以得到最小值 $x_0 = 0$, 因此在 $x_1 = \pm 1, x_2 = \pm 1$ 可以达到. 注意从集合 $\{0,1\}$ 中我们找不到与 M 的最大值有关的任何信息, 因为 M 的最大值并不存在, 上述方法也不能再被应用.

换个角度, 我们也可以用有限核定理或是定理 5.5.37 来确定最小值. 易知

$$\mathrm{Zero}_{\mathbf{R}}(h_0) = \bigcup_{k=1,\cdots,5} \mathrm{Zero}_{\mathbf{R}}(CS'_k/*), \tag{8.2.47}$$

其中 * 表示相关初式 - 隔离子乘积, 且

$$\left.\begin{aligned}
&CS'_1 = \{h_0\},\\
&CS'_2 = \{x_1^2 * (x_1^2 - 3)^2 + 4 * (1 - x_0), 2 * x_2^2 + x_1^2 - 3\},\\
&CS'_3 = \{x_0 - 1, x_1\},\\
&CS'_4 = \{x_0 - 1, x_2\},\\
&CS'_5 = \{x_0, x_1^2 - 1, x_2^2 - 1\}.
\end{aligned}\right\} \tag{8.2.48}$$

在 (8.2.47) 右边, 前两个零点集对有限核集没有什么贡献, 而其他三个零点集则分别给出三个值 1, 1, 0. 由此可得

$$K = \mathrm{Ker}\{x_0, \mathbf{R}^3, h_0\} = \{0,1\}. \tag{8.2.49}$$

因此, 我们又得到

$$\mathrm{Least}(M) = \mathrm{Least}\{x_0, \mathbf{R}^3, h_0\} = \mathrm{Least}\{K\} = 0, \tag{8.2.50}$$

而且最小值 $x_0 = 0$ 源于 CS'_5, 于是它在点 $x_1 = \pm 1, x_2 = \pm 1$ 处达到. □

<u>代数不等式和三角不等式的证明</u>

我们的方法可以证明一些在数学中频繁出现的代数、三角和几何不等式. 几何不等式的例子已在 §7.4 中给出. 以下为一些很简单的代数和三角不等式的例子, 用以说明. 更多的例子参见 [WDK1] 以及作者的相关文献.

例 8.2.2 对于 $a, b, c > 0$ 有

$$(b + c) * (c + a) * (a + b) \geq 8 * a * b * c. \tag{8.2.51}$$

而且, 对任一个三元组 $a = b = c > 0$ 等式成立.

证明 将 a,b,c 重新写做 x_1,x_2,x_3, 运用 Seidenberg 的技巧, 引入 y_1,y_2,y_3, 使得 $h_i=0,i=1,2,3$, 其中

$$h_i = y_i^2 * x_i - 1,\ i=1,2,3. \tag{8.2.52}$$

通过用 $h_0=0$ 定义 x_0, 其中

$$h_0 = y_1^2 * y_2^2 * y_3^2 * (x_2+x_3)*(x_3+x_1)*(x_1+x_2) - x_0, \tag{8.2.53}$$

则, 我们遇到问题 Ineq, 其中 D: $0 \le x_i < +\infty$, $0 \le y_i < +\infty$, 且

$$f = x_0,\ g=1,\ HS=\{h_0,h_1,h_2,h_3\}.$$

由 h_i $(i=1,2,3)$ 可知, x_0 的最小值必定存在. 因此我们的方法可以用于最小值的情形. 我们要证明的不等式等价于证明由 $h_0=0$ 确定的 x_0 的最小值为 8. 用 Lagrange 乘子 λ_i, $i=0,1,2,3$, Lagrange 多项式可由下式给出:

$$L = x_0 + \lambda_0 * h_0 + \lambda_1 * h_1 + \lambda_1 * h_1 + \lambda_3 * h_3. \tag{8.2.54}$$

Lagrange 多项式集由下式给出:

$$LS = \left\{\frac{\partial L}{\partial x_0}, \frac{\partial L}{\partial x_i}, \frac{\partial L}{\partial y_i}, h_0, h_i \mid i=1,2,3\right\}.$$

变量序为

$$x_0 \prec x_1 \prec x_2 \prec x_3 \prec y_1 \prec y_2 \prec y_3 \prec \lambda_1 \prec \lambda_2 \prec \lambda_3,$$

易知 LS 的特征列集由 9 个多项式组成, 前 3 个特征多项式如下:

$$\left.\begin{aligned} C_1 &= x_0*(x_0-8),\\ C_2 &= x_2 - x_1,\\ C_3 &= x_3 - x_1. \end{aligned}\right\} \tag{8.2.55}$$

因为 $h_i=0$, $i=1,2,3$, $C_1=0$ 的解为 $x_0=0$ 是不可能的. $x_1=x_2=x_3$ (>0) 取任意值时, 必有 x_0 的最小值是 8. □

我们基于 §5.5 有限核定理的方法也可以用来证明三角不等式. 下面是用该方法证明的最简单的例子之一. 其他一些用这种方法证明的三角不等式的例子, 请参考王定康的博士论文 [WDK1].

例 8.2.3 (Sine-Sum 定理) 对三角形 ABC, 有

$$\sin\ A + \sin\ B + \sin\ C \le \frac{3}{2} * \sqrt{3}. \tag{8.2.56}$$

证明 令

$$\left.\begin{array}{l}\sin\ A = x_1,\ \sin\ B = y_1, \sin\ C = z_1,\\ \cos\ A = x_2,\ \cos\ B = y_2, \cos\ C = z_2,\end{array}\right\} \tag{8.2.57}$$

则有 $HS = 0$, 其中 $HS = \{h_1, \cdots, h_5, h_0\}, h_i$ 如下所示:

$$\left.\begin{array}{l}h_1 = x_1^2 + x_2^2 - 1,\\ h_2 = y_1^2 + y_2^2 - 1,\\ h_3 = z_1^2 + z_2^2 - 1,\\ h_4 = x_1 * y_2 + x_2 * y_1 - z_1,\\ h_5 = x_2 * y_2 - x_1 * y_1 + z_2,\\ h_0 = x_0 - (x_1 + y_1 + z_1).\end{array}\right\} \tag{8.2.58}$$

由 h_1, h_2, h_3 知, x_0 的最大值与最小值都存在, 但是我们感兴趣的仅是如下所示区域中的 x_i, y_i, z_i 的值:

$$D : 0 \leq x_1, y_1, z_1 \leq +1,$$

变量序为

$$x_0 \prec x_1 \prec y_1 \prec z_1 \prec x_2 \prec y_2 \prec z_2.$$

我们需考虑在约束条件 $HS = 0$ 下, 确定 D 中 x_0 的最大值. $\mathrm{Zero}_{\mathbf{R}}(HS)$ 是 29 个零点集 $\mathrm{Zero}_{\mathbf{R}}(CS_k/ISP_k)(k = 1, \cdots, 29)$ 的并, 明确的表示式参见王定康的博士论文 [WDK1]. 经证实大多数的解对有限核集毫无意义. 根据有限核定理可以得到核集

$$K = \{0, 2, \sqrt{2} \pm 1, \frac{3}{2} * \sqrt{3}\}. \tag{8.2.59}$$

由特征集

$$\begin{aligned}CS = \{4 * x_0^2 - 27,\ 3 * x_1 - x_0,\ 3 * y_1 - x_0,\ 3 * z_1 - x_0,\\ 2 * x_2 - 1,\ 2 * y_2 - 1,\ 2 * z_2 - 1\}\end{aligned} \tag{8.2.60}$$

可知 x_0 的最大值, 即 $\sin\ A + \sin\ B + \sin\ C$ 的最大值是 $\frac{3}{2} * \sqrt{3}$, 这样 x_1, y_1, z_1 的值均等于 $\frac{1}{2} * \sqrt{3}$, x_2, y_2, z_2 的值都等于 $\frac{1}{2}$. 于是, (8.2.56) 是正确的, 等式成立当且仅当三角形为等边三角形. 注意最小值 $-\frac{3}{2} * \sqrt{3}$ 是毫无意义的, 因为它对应于 $A = x_1 = -\frac{1}{2} * \sqrt{3} < 0$.

<u>四次问题和椭圆问题</u>

这两个问题已经被不少人广泛地研究过. 参见文献 [A-M], [C-H], [Mig] 等. 用我们的方法解决第一个问题时，需引用以下引理:

引理 8.2.4 令方程

$$c_0 * y^3 + c_1 * y^2 + c_2 * y + c_3 = 0 \quad (c_0 > 0) \tag{8.2.61}$$

的判别式为 Δ. 满足方程的 y 的值为正的充分必要条件是下列条件 (1) 或 (2) 成立:

(1) $\Delta < 0$ 且 $c_3 < 0$.

(2) $\Delta \geq 0$ 且 $c_1 < 0$, $c_2 > 0$, $c_3 < 0$.

满足方程 (8.2.61) 的 y 非负的充分必要条件是上述条件 (1) 或 (2), 或是以下条件 (3) 成立:

(3) $c_3 = 0$, $c_1 \leq 0$, $c_2 \geq 0$, 且 $c_1^2 - 4 * c_0 * c_2 \geq 0$.

证明 参见 [Fr], p.188. □

例 8.2.5 (四次问题) 考虑实四次方程

$$y = x^4 + p * x^2 + q * x + r. \tag{8.2.62}$$

求 p, q, r 需满足怎样的条件才能使得 y 总是 ≥ 0 或 > 0.

我们的方法导出考虑一个 Ineq 问题，其中

$$D = \mathbf{R}^2(x, y),\ f = y,\ g = 1,$$

且

$$h_1 = -y + x^4 + p * x^2 + q * x + r.$$

显然 y 的最小值存在，可采用 5.5.37 或 5.5.38 中的方法. 易见对应集 $LJVal$ 为三次方程 (8.2.61) 的实零点集，其中

$$\left.\begin{aligned}
&c_0 = 256,\\
&c_1 = 128 * (p^2 - 6 * r),\\
&c_2 = 16 * (p^4 - 16 * p^2 * r + 48 * r^2 + 9 * p * q^2),\\
&c_3 = -16 * p^4 * r + 4 * p^3 * q^2 + 128 * p^2 * r^2\\
&\qquad -144 * p * q^2 * r + 27 * q^4 - 256 * r^3.
\end{aligned}\right\} \tag{8.2.63}$$

(8.2.61) 的判别式 Δ 由下式给出:

$$\Delta = -\, q^2 * (8 * p^3 + 27 * q^2)^3. \tag{8.2.64}$$

四次问题就等价于确定当 c_i 满足何种条件时, (8.2.61) 有非负根或者只有正根, 详细条件由引理 8.2.4 确定

例 8.2.6 (椭圆问题) 考虑单位圆 $C: x^2+y^2=1$, 和椭圆 $E(x,y)=0$, 其中

$$E = a_1 * x^2 + 2 * a_2 * x * y + a_3 * y^2 + 2 * a_4 * x + 2 * a_5 * y + a_6. \tag{8.2.65}$$

为确保 $E=0$ 为真正的椭圆, 我们加上以下不等式条件:

$$a_2^2 - a_1 * a_3 < 0,\ a_1 > 0,\ a_3 > 0.$$

问题是确定使椭圆始终完全在 C 的内部时, a_i 所满足的条件 (可以相切或不相切). 这个问题也和四次问题一样被广泛地研究, 主要限于 $a_2=a_5=0$ 的情形, 即椭圆的一个轴与 X 轴重合. 如果没有这样的限制, 用我们的方法就会导出考虑一个 Ineq 问题, 其中

$$D = \mathbf{R}^3(x,y,r),\ f=r,\ g=1,$$

且

$$h_1 = E(x,y),\ h_2 = x^2+y^2-r.$$

由于 $E=0$ 是一个椭圆, 所以 f 的最大值显然存在, 可再次应用定理 5.5.37 或 5.5.38. 除了一些在此处我们没有明确给出的退化情形可以去掉以外, 我们还可以去掉 E 为圆或是 $a_2^2+(a_1-a_3)^2=0$ 这样无意义的情形. 我们很容易发现在一般情况下, r 的最大值可能就是 r 的四次方程 $Q(r)=0$ 的最大实根. 四次方程 Q 的所有系数多项式为 a_i 且项数 $=123$. 最初始的问题等价于根据是否相切, 找到关于系数 a_i 的条件, 使得 $Q(r)=0$ 没有 >1 或 ≥ 1 的实根. 后一个问题简化为例 8.2.5, 从而得到解决. 参见图 8.3.

<u>非线性规划问题</u>

显然可以用我们的方法解决非线性规划中目标函数和约束条件均为多项式的问题. 以下是一个最简单的示例之一. 更多的例子参见文献 [WTJ1].

例 8.2.7 (非线性规划问题) 最小化

$$f = 1000 - x_1^2 - 2 * x_2^2 - x_3^2 - x_1 * x_2 - x_1 * x_3, \tag{8.2.66}$$

其中 f 满足下列约束条件:

$$\left.\begin{aligned} h_1 &= x_1^2 + x_2^2 + x_3^2 - 25 = 0, \\ h_2 &= 8 * x_1 + 14 * x_2 + 7 * x_3 - 56 = 0, \end{aligned}\right\} \tag{8.2.67}$$

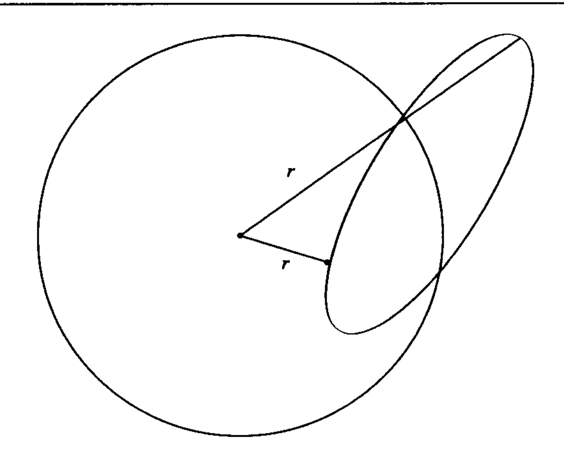


图 8.3 椭圆问题

和

$$x_i \geq 0,\ i = 1, 2, 3. \tag{8.2.68}$$

首先注意到由 (8.2.67) 的第一个条件可知 f 的最小值一定存在. 将 (8.2.68) 中定义的区域分为 8 个开域, 每个区域中 $x_i > 0$ 或 $= 0$. 易知所有的 $x_i > 0$ 时, 开域 D_1 中唯一的 E- 零点是

$$Z_1 = (3.512,\ 0.217,\ 3.552). \tag{8.2.69}$$

对于其他的开域, 仅在由 $x_1 = 0$ 或 $x_1 > 0$ 和 $x_2 > 0$, $x_3 > 0$ 定义的开域 D_2 或 D_3 上, 有两个其他的 E- 零点, 即

$$Z_2 = \left(0,\ \frac{32 - 2\sqrt{61}}{10},\ \frac{8 + 2\sqrt{61}}{5}\right) \text{ 和 } Z_3 = \left(\frac{63}{13}, \frac{16}{13, 0}\right) \tag{8.2.70}$$

相应的 E- 值分别为

$$f(Z_1) \approx 961 \text{ 和 } f(Z_2) \approx 972. \tag{8.2.71}$$

满足所述条件的 f 的最小值逼近 961, 它的取值点为 (8.2.69) 给出的点 Z_1. 细节参见上文引用的文献 [WTJ1].

<u>一个碰撞问题</u>

下面考虑一个 Collins 和 Hong 已经研究过的在某种特殊情形下的碰撞问题, 参见 [C-H].

例 8.2.8 (碰撞问题) 假设两辆形状已给定的车按已知的速度 $v_1 > 0$ 和 $v_2 > 0$ 分别沿着 X 轴和 Y 轴的正方向移动. 确定这两辆车是否会碰撞, 以及发生第一次碰撞的时间和地点.

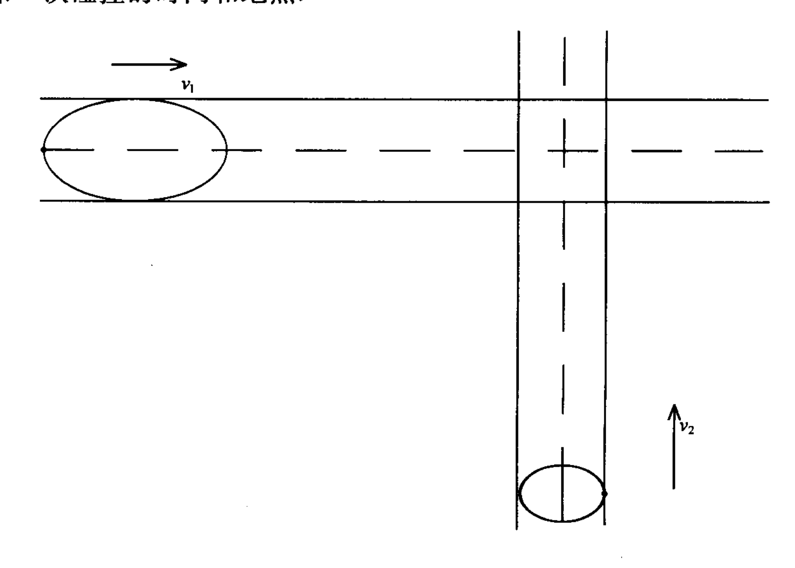


图 8.4 碰撞问题

令两辆车的初始位置分别为

$$f_1(x,y)=0,$$

和

$$f_2(x,y)=0.$$

则该问题可看作一个 Ineq 问题, 其中

$$D=\{t>0\}\subset \mathbf{R}^3(t,x,y),\ f=t,\ g=1,$$

$$h_1=f_1(x-v_1*t,y),\ h_2=f_2(x,y-v_2*t).$$

特别地, 考虑两辆车形状均为由 $(c_1<0,c_2<0)$ 给定的椭圆形的情形:

$$f_1(x,y)=b_1^2*(x-c_1)^2+a_1^2*y^2-a_1^2*b_1^2,$$
$$f_2(x,y)=b_2^2*x^2+a_2^2*(y-c_2)^2-a_2^2*b_2^2.$$

在 a_i,b_i,c_i, 和 v_i 取一般值的情况下, 我们的方法将产生一个关于 t 的次数为 8, 项数 $=696$ 的多项式. 去掉那些无意义的情况, 当且仅当方程有正根时, 两

辆车会碰撞. 如果替换 a_i, b_i, c_i, 和 v_i 的数值解 (满足一般条件), 很容易确定第一次碰撞的时间和地点. 进一步考虑两辆车形状相同的特殊情况, 即

$$a_1^2 * b_2^2 = a_2^2 * b_1^2,$$

特别是当两辆车的形状都为圆时, 碰撞发生的情况. 我们可以得到一个关于 t 的线性的和二次的方程组. 可能发生碰撞的条件以及第一次碰撞发生的时间和地点, 都可以用关于 a_i, b_i, c_i, 和 v_i 的显式方程表示出来. 细节参见文献 [WTJ2]. 亦可参见图 8.4.

§8.3 四连杆机构设计方面的应用

四连杆机构设计方面的问题

四连杆机构的描述已经在 §8.1 定义 8.1.14 和例 8.1.15 中给出. 一个给定平面上的四连杆机构有 9 个参数: 4 个参数固定它的固定末端 $A = (a_1, a_2), B = (b_1, b_2)$ 的位置; 3 个参数 p, q, r 代表 $|AU|$, $|BV|$, $|UV|$ 的长度; 2 个参数固定三角形 UVZ : 一个是三角形 UVZ 边 UV 上的高 h, 一个是边 UZ 到 UV 上的正交投影 s, 参见 §8.1. 这样, 四连杆机构设计的第一个问题如下:

问题 L1 已知连杆机构平面上的连结点 Z 的 9 个位置, 在这个平面上确定这个四连杆机构.

连结点 Z 记为 (x, y), 在例 8.1.15 我们已经确定了 Z 的用上面的那 9 个参数表示的方程 $H(x, y) = 0$. 设 Z 的 9 个已知位置的坐标为 $Z_i = (c_i, d_i)$, 则

$$H_i \equiv H(c_i, d_i) = 0,\ i = 1, \cdots, 9,$$

给出关于 9 个变量 $a_1, b_1, a_2, b_2, p, q, r, h, s$ 的 9 个方程. 求解这样一个复杂的多项式方程组超出了现在的多项式方程组求解的特征列方法的能力, 尽管原理上我们总可以这样做. 即使我们采用如 §8.1 所示的用复变量代替实参数, 这样决定未知参数的方程会大大简化, 好像求解依然超出了我们的 *符号* 方法的能力. 在有数据的具体情形, 我们在 §6.2 所描述的混合方法可能被应用, 但是仍需要试验. 但是, 尽管如此, 仍然有一些在技术上很重要的问题能被我们的 *符号* 方法完全解决. 下面就是一例.

已知 5 个连结杆平面位置的四连杆机构设计

我们不是研究问题 L1, 而是研究与问题 L1 同等重要的四连杆机构设计的问题:

问题 L2　已知移动连结平面在固定连结平面的 5 个平面位置，设计此四连杆机构.

在 1995 年关蔼文和刘惠林给出了解决上述问题 L2 的一个简单方法，先把问题简化成一组多项式方程组，然后应用我们的一般方法求解，参见他们的文章 [L-G]. 经证实，问题 L2 已经有基于 Burmester 点几何理论的经典解法，它也是把问题简化成一组多项式方程组. 比较这两种方法作者对于上面的第二种方法做了一些简化，不需要很多几何知识. 我们在下面将列出这三种方法.

四连杆机构的 Burmester 几何理论回顾

记号 8.3.1　$E :=$ 四连杆机构 $AUVB$ 的固定平面. $E_i(i=0,1,\cdots,4) :=$ 固定平面 E 上的 5 个移动连结平面. $U_iV_i(i=0,1,\cdots,4) :=$ 在移动连结平面 E_i 上的 5 个移动连结杆. $P_{ij}=P_{ji}(i,j=0,1,\cdots,4,\ i\neq j) :=$ 从平面 E_i 到平面 E_j 的旋转极点. $\theta_{ij}=-\theta_{ji} \bmod 2*\pi(i,j=0,1,\cdots,4,\ i\neq j) :=$ 平面 E_i 到平面关于 P_{ij} 的旋转角.

定义 8.3.2　如果当平面 E_i 移到平面 E_j 时点 P_i 移到 P_j, 则称分别在移动平面 E_i,E_j 上的两个点 P_i,P_j 是 *相关的*.

定义 8.3.3　分别在移动平面 E_i, E_j, E_k, E_l 上的 4 个相关点所在圆的圆心称为相对于四个不同的移动平面 E_i, E_j, E_k, E_l 的 *中心点* C_{ijkl}.

定义 8.3.4　相对于移动平面 E_i,E_j,E_k,E_l 的所有中心点 C_{ijkl} 的轨迹定义为 *中心曲线* Γ_{ijkl}.

定义 8.3.5　固定平面 E 上的对 $P_{ik}P_{il}$ 和 $P_{jk}P_{jl}$ 的张角相同的，且使得

$$\left.\begin{aligned} &<(PP_{ik},PP_{il})=<(PP_{jk},PP_{jl}),\\ \text{或}\quad &\\ &<(PP_{ik},PP_{jk})=<(PP_{il},PP_{jl}) \end{aligned}\right\} \tag{8.3.72}$$

的点称为相对于 4 个不同的移动平面 E_i,E_j,E_k,E_l 的 *极点* $P_{ij,kl}$.

注释 8.3.6　这一节的所有角是如 §7.2 所定义的有向角. 除非另作声明，关于有向角的所有方程，如上面的 (8.3.72) 和下面的 (8.3.73), 理解为模 π 相同.

注释 8.3.7　对移动平面 $E_i(i=0,1,\cdots,4)$ 的已知位置，极点 P_{ij} 和角 $\theta_{ij} \bmod 2*\pi(i,j=0,1,\cdots,4,i\neq j)$ 都是已知的.

定义 8.3.8　相对于移动平面 E_i,E_j,E_k,E_l 的所有极点 $P_{ij,kl}$ 的轨迹定义为相对于这 4 个不同的移动平面的 *极点曲线* $\Pi_{ij,kl}$.

命题 8.3.9 对 $i \neq j$, 点 P_{ij}, A 在 U_iU_j 的垂直平分线上，因此

$$<(P_{ij}U_i, P_{ij}A) = \frac{\theta_{ij}}{2}.$$

命题 8.3.10 对不同的移动平面 E_i, E_j, E_k:

$$<(P_{ij}P_{ik}, P_{ij}P_{jk}) = \frac{\theta_{ij}}{2}. \tag{8.3.73}$$

命题 8.3.11 (Burmester) 中心曲线 Γ_{ijkl} 和极点曲线 $Pi_{ij,kl}$ 是相互重合的三次曲线.

命题 8.3.12 (Burmester) 中心曲线 Γ_{ijkl} 或极点曲线 $\Pi_{ij,kl}$ 都经过 6 个极点 P_{ij}, P_{ik}, P_{il}, P_{jk}, P_{jl}, P_{kl} 且过两个在无穷远的圆点.

有关这些命题的证明可以参考有关机械或连杆机构的几何理论的经典教材，例如 [Bey], 或者 [LXY].

基于 Burmester 几何理论的问题 L2 的解法

显然，固定端 A 是一个中心点，因为连接点 $U_i(i = 0, 1, \cdots, 4)$ 是移动平面 E_i 上的相关点，它们都在同一个以 A 为中心的圆上，所以 A 可以由两条三次曲线 $\Pi_{01,23}, \Pi_{01,24}$ 相交来确定. 因为两条三次曲线一般情况下相交有 9 个点，3 个极点 P_{01}, P_{02}, P_{12}, 2 个对我们的问题无关的在无穷远的虚圆点，这样我们希望对位置 A, 不管实数或复数有 4 个解. 这就形成了求解问题 L2 的理论基础. 参看图 8.5.

取坐标使得

$$P_{ij} = (p_{ij}, q_{ij}),\ i, j = 0, 1, \cdots, 4,\ i \neq j,$$

$$A = (x, y).$$

如注释 8.3.7 所示， p_{ij}, q_{ij} 已知，则从 (8.3.72) 知，对 $(ij, kl) = (01, 23)$, $(01, 24), (01, 34)$ 有:

$$<(AP_{02}, AP_{12}) =< (AP_{03}, AP_{13}) =< (AP_{04}, AP_{14}). \tag{8.3.74}$$

用 ω 记公共角，并设 $\tan\omega = w$, 则得到三个方程:

$$\begin{aligned} & w((x^2+y^2) - x*(p_{0j}+p_{1j}) - y*(q_{0j}+q_{1j}) + (p_{0j}*p_{1j}+q_{0j}*q_{1j})) \\ = \ & x*(q_{0j}-q_{1j}) + y*(p_{1j}-p_{0j}) + (p_{0j}*q_{1j}-p_{1j}*q_{0j}), \quad j = 2, 3, 4. \end{aligned} \tag{8.3.75}$$

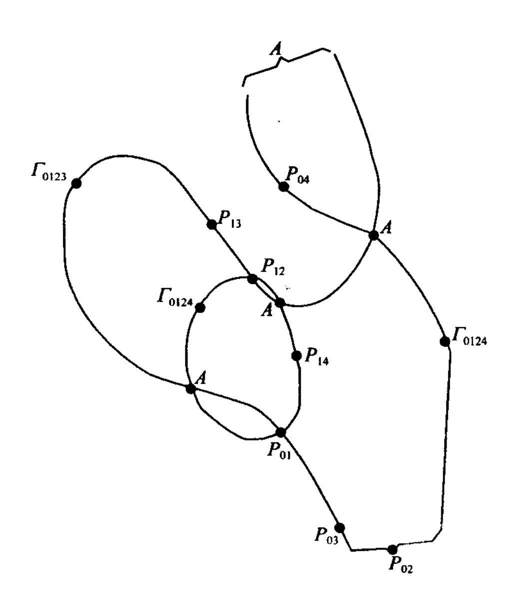


图 8.5　基于 Burmester 几何理论的问题 L2 的解法

方程组 $(8.3.75)_j (j=2,3,4)$ 是关于三个未知量 w,x,y 的三个方程. 未知量的序如下:

$$w \prec x \prec y.$$

用我们的一般方法得到一个特征列, 其中第一个是关于 w 的 4 次多项式, 剩下的 2 个分别是关于首变量 x,y 的线性多项式. 这就是问题 L2 的关于末端 A 的一个解. 由于等式 $(8.3.75)_j$ 的一些特性, 我们也可以用下面更直接的方式解方程.

$(8.3.75)_2$ 减去 $(8.3.75)_3$, $(8.3.75)_4$, 我们就得到两个方程

$$(\alpha_{i1} * w + \alpha_{i2}) * x + (\alpha_{i3} * w + \alpha_{i4}) * y(\alpha_{i5} * w + \alpha_{1i}) = 0, \quad i = 1,2, \quad (8.3.76)$$

其中所有的 α_{ik} 是关于 p_{ij}, q_{ij} 的定义多项式. 解出方程 $(8.3.76)_1$, $(8.3.76)_2$ 中的 x,y, 我们得到下面形式的方程:

$$\left.\begin{aligned} x &= \frac{\beta_{11} * w^2 + \beta_{12} * w + \beta_{13}}{\beta_{14} * w^2 + \beta_{15} * w + \beta_{16}}, \\ y &= \frac{\gamma_{11} * w^2 + \gamma_{12} * w + \gamma_{13}}{\gamma_{14} * w^2 + \gamma_{15} * w + \gamma_{16}}, \end{aligned}\right\} \quad (8.3.77)$$

其中所有的 β 和 γ 是关于 α 的定义多项式，也就是关于 p 和 q 的定义多项式. 现在把 (8.3.77) 中的 x,y 的最后表达式代入 (8.3.75) 中的任何一个，我们将得到同样的次数为 4 的关于 w 的方程，其系数是关于 β, γ, p 和 q 的定义多项式，这样也就是所有关于 p 和 q 的定义多项式.

从关于 w 的最后一个方程和关于 x,y 的等式 (8.3.77), 我们看到一般情况下对固定端 $A=(x,y)$ 有四个解, 实解或者虚解, 记为 $A_i=(x_i,y_i), i=1,\cdots,4$. 现在固定端为 B 的情形和 A 的情形是一样的，所以 4 个点 A_i 可以等价的移到 B. 因此一般情况下有 6 对 (A,B), 或者实或者虚. 对这样的任意的一对，当是实的时，连接点 U_0,V_0 可由命题 8.3.9 确定，由此四连杆机构可以完全确定. 我们看到给定 5 个移动连结平面位置的四连杆机构实际可能解一般至多是 6 个. 当然，在退化情形下可能无解或者有无穷多解. 无论如何对每一个具体情形可以给出具体分析.

问题 L2 的一个简化解

前面的经典解法需要很多有关连杆机构运动的几何知识. 下面我们提出一种简化解法，它只要求一些基本的几何知识.

如同注释 8.3.6, 从平面 E_0 旋转到 E_j 的极点 P_{0j} 和角 $\theta_{0j} \bmod 2*\pi$ 都是已知的. 由注释 6.3.4, P_{0j} 和末端 A 都在 U_0U_j 的垂直平分线上. 不考虑无意义的和极少可能出现的退化情形 $P_{0j}=U_0$ 或者 $P_{0j}=A$, 我们有

$$<(P_{0j}U_0,P_{0j}A)=\frac{1}{2}<(P_{0j}U_0,P_{0j}U_j)=\frac{1}{2}*\theta_{0j},\ j=1,\cdots,4. \tag{8.3.78}$$

设 $\tan\left(\frac{1}{2}*\theta_{0j}\right)=t_j$ 且取坐标使得

$$A=(x,y),\ U_0=(x_0,y_0),\ P_{0j}=(c_j,d_j),\ j=1,\cdots,4,$$

其中 c_j,d_j,t_j 已知，而 x,y,x_0,y_0 待确定. 见图 8.6.

从 (8.3.78) 我们得到方程 $P_j=0,\ j=1,\cdots,4$, 这里

$$\begin{aligned}P_j=&(y_0*x-x_0*y)-(y_0*y+x_0*x)*t_j\\&+y_0*(t_j*d_j-c_j)+x_0*(t_j*c_j+d_j)\\&+y*(t_j*d_j+c_j)+x*(t_j*c_j-d_j)-t_j*(c_j^2+d_j^2).\end{aligned} \tag{8.3.79}$$

4 个多项式 P_j 关于四个未知量 y_0*x-x_0*y, y_0*y+x_0*x, y_0 和 x_0 是线性

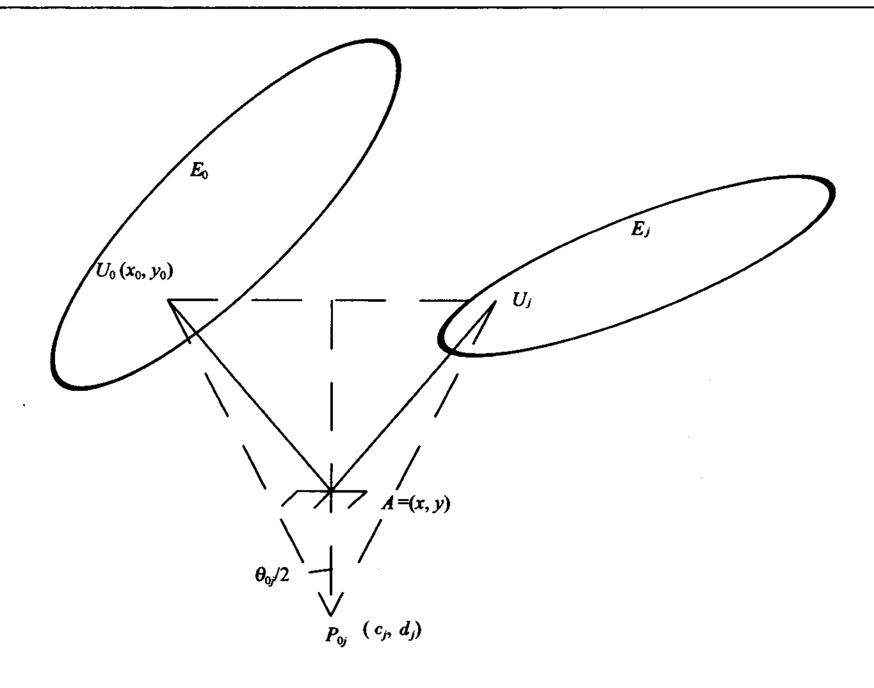


图 8.6 问题 L2 的一个简化解

的. 记四个未知量的系数矩阵的行列式为 D, 则求解方程 $P_j = 0$, 我们得到

$$\left.\begin{aligned}&D * (y_0 * x - x_0 * y) = r_{11} * x + r_{12} * y + r_{10},\\&D * (y_0 * y + x_0 * x) = r_{21} * x + r_{22} * y + r_{20},\\&D * x_0 = r_{31} * x + r_{32} * y + r_{30},\\&D * y_0 = r_{41} * x + r_{42} * y + r_{40},\end{aligned}\right\} \tag{8.3.80}$$

其中 D 和 r 等是关于参数 t_j, c_j, d_j 的所有定义多项式. 用 (8.3.80) 的最后两个方程的右侧的表达式值取代前两个方程中的 $D * x_0, D * y_0$, 我们得到下面的两个方程:

$$s_{i1} * y^2 + (s_{i2} * x + s_{i3}) * y + (s_{i4} * x^2 + s_{i5} * x + s_{i6}) = 0,\ i = 1, 2, \tag{8.3.81}$$

其中所有的 s 等是关于 r 等的确定的多项式, 因此也是关于 t_j, c_j, d_j 的确定的多项式. 取变量序为

$$x \prec y \prec x_0 \prec y_0.$$

多项式集合 $PS = \{P_1, \cdots, P_4\}$ 的一个特征集可由 $C_1, \cdots, C_4$ 这 4 个多项式组成, 其中 C_1 是关于 x 的一个 4 次多项式, C_2, C_3, C_4 关于主变元 y, x_0, y_0 是

线性的，这里 C_3, C_4 可以从 (8.3.80) 中最后两个方程导出. 多项式 $C_1, \cdots, C_4$ 的系数都是关于未知元 t_j, c_j, d_j 的确定的多项式. 由此可知一般对 (A, U_0) 至多有 4 个实解. 同前所述，我们可以取一对这样的实解来形成一个四连杆机构 AU_0V_0B, 它在一般情况下至多有 6 个.

<u>问题 L2 的关 - 刘解法</u>

问题 L2 的关 - 刘方法同前面的相比仍然需要较少的一些有关连杆运动的几何知识，参看他们合作的文章 [L-G]. 他们的方法如下：在移动平面 E_0 上取一任意点 P_0 以及在移动平面 $E_j(j=1,\cdots,4)$ 上的相关点 P_j. 作如图 8.7 的平行四边形 $U_0U_jP_jP_j'$.

点 P_0, P_j 已知，所以向量 $\overrightarrow{P_0P_j}$ 也是已知. 点 U_0, U_j, A 未知且有待确定. 但是显然 U_0, U_j 如同 P_0, P_j 一样是相关点，所以角 $<(U_0P_0, U_jP_j)=\alpha_j$ 事实上是知道的，设未知角 $<(AU_0, AU_j)=\phi_j$. 现在取坐标使得

$$\overrightarrow{AU_0}=(x_1,x_2),\ \overrightarrow{U_0P_0}=(x_3,x_4),\ \overrightarrow{P_0P_j}=(c_j,d_j),\ j=1,\cdots,4,$$

则我们只需要用 ϕ_j, c_j, d_j 确定 x_1, x_2, x_3, x_4, 就可以确定 A, U_0, 由此如上两个解法一样确定一个四连杆机构.

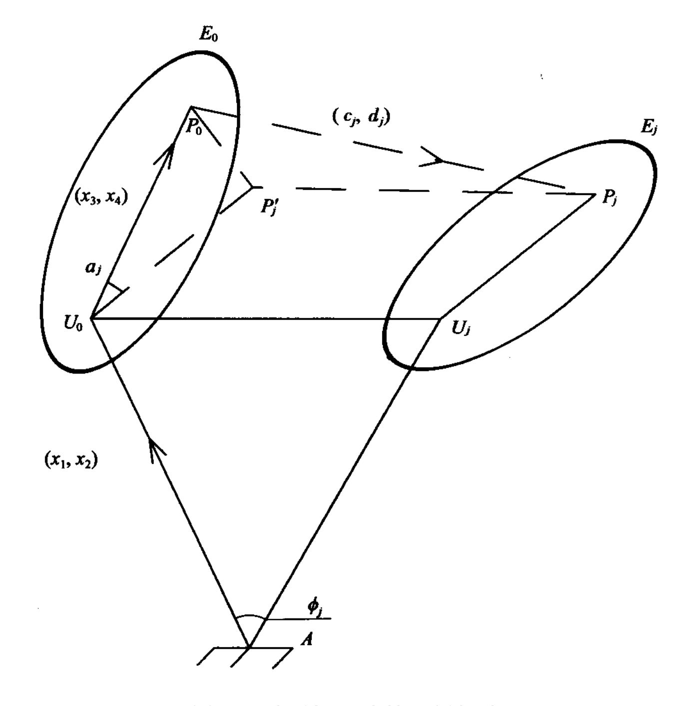


图 8.7 问题 L2 的关 - 刘解法

为了用 ϕ_j, c_j, d_j 确定 $x_1, \cdots, x_4$, 从图 8.7, 我们看到

$$\left.\begin{aligned}
&\overrightarrow{P_0P_j} = \overrightarrow{P_0P_j'} + \overrightarrow{P_j'P_j} = \overrightarrow{P_0P_j'} + \overrightarrow{U_0U_j},\\
&\overrightarrow{P_0P_j'} = \overrightarrow{U_0P_j'} - \overrightarrow{U_0P_0} = \overrightarrow{U_0P_0} * (R_{\alpha_j} - 1), \qquad j = 1, \cdots, 4.\\
&\overrightarrow{U_0U_j} = \overrightarrow{AU_j} - \overrightarrow{AU_0} = \overrightarrow{AU_0} * (R_{\phi_j} - 1),
\end{aligned}\right\} \tag{8.3.82}$$

在 (8.3.82) 中 R_{α_j}, R_{ϕ_j} 分别表示角 a_j, ϕ_j 关于 U_0, A 的旋转. 设 $\cos\phi_j = y_j$, $\sin\phi_j = z_j$, $\cos\alpha_j = a_j$, $\sin\alpha_j = b_j$, 则我们有下面的 12 个方程 ($j = 1, \cdots, 4$):

$$\left.\begin{aligned}
&x_1 * (y_j - 1) - x_2 * z_j + x_3 * (a_j - 1) - x_4 * b_j - c_j = 0,\\
&x_1 * z_j + x_2 * (y_j - 1) + x_3 * b_j + x_4 * (a_j - 1) - d_j = 0,\\
&\qquad y_j^2 + z_j^2 - 1 = 0.
\end{aligned}\right\} \tag{8.3.83}$$

在 (8.3.83) 中, 所有的 x, y, z 都是未知的参数, 而 a, b, c, d 都是已知的参数, 且满足条件 $a_j^2 + b_j^2 = 1$.

将未知变量排序如下:

$$x_1 \prec x_2 \prec x_3 \prec x_4 \prec y_1 \prec z_1 \prec \cdots \prec y_4 \prec z_4.$$

用一种显然的方式消去变量 y_j, z_j, 我们得到一个关于 $x_j (j = 1, \cdots, 4)$ 的多项式集 $PS = \{P_1, \cdots, P_4\}$,

$$\begin{aligned}
P_j = & f_{j0} * (x_3^2 + x_4^2)\\
&+ x_4 * (f_{j1} * x_1 + f_{j2} * x_2 + f_{j3})\\
&+ x_3 * (f_{j4} * x_1 + f_{j5} * x_2 + f_{j6})\\
&+ (f_{j7} * x_1 + f_{j8} * x_2 + f_{j9}), \quad j = 1, \cdots, 4,
\end{aligned} \tag{8.3.84}$$

其中所有的 f 都是关于已知参数 a, b, c, d 等的确定的多项式. 由我们的多项式方程求解的一般方法, 最后得到一个特征列 $CS = \{C_1, \cdots, C_4\}$, C_1 是仅关于 x_1 的一个 4 次多项式. C_2, C_3, C_4 分别是关于 x_2, x_3, x_4 的线性多项式. 同前, 一般情况下对 A, U_0 至多有 4 个实解, 结合它们中两个得到一般情况下对四连杆机构 AU_0V_0B 最多有 6 个解.

§8.4 在计算机辅助几何设计的曲面拼接问题中的应用

取 $\mathbf{K}, X = (x_1, \cdots, x_n)$ 如前所述.

计算机辅助几何设计 (CAGD) 的曲面拼接问题

本节我们将对下面的 CAGD 中的曲面拼接问题给出一个一般性方法.

问题 SF 给定 $\mathbf{R}^3$ 空间三条实不可约代数曲线 C_i, C_j, C_k, 其中 $i \in I, j \in J, k \in K$, I, J, K 是有限集. 同时给定两个分别包含 C_j, C_k 的实不可约代数曲面 $S_j, S_k (j \in J, k \in K)$. 确定一个具有给定幂次 m 的实不可约代数曲面 S, 满足下述条件:

1. 对 $i \in I, j \in J, k \in K$, S 包含所有曲线 C_i, C_j, C_k.
2. 对 $j \in J$, $k \in K$, S 分别沿曲线 C_j, C_k 与 S_j, S_k 光滑拼接. 更准确地说, 对 C_j 或 C_k 上每一关于 C_j, S_j 或 C_k, S_k 的正则点, 所求曲面 S 在此点也是正则的. 进一步, S 与 S_j 或 S 与 S_k 在此点将具有相同切平面.
3. 对任一 $k \in K$, S 沿曲线 C_k 具有与 S_k 相同的曲率. 准确地说, 对 C_k 上每一关于 C_k, S_k 的正则点, 曲面 S 与 S_k 在此点不仅具有相同切平面而且具有相同的 (Gauss) 曲率.

我们也可用其他更严格要求来代替条件 3, 对其我们就不再论述.

注释 8.4.1 实曲线, 实曲面及正则点的准确含义, 下面将具体陈述.

注释 8.4.2 对要求 (1),(2) 及其他更严格光滑要求的问题, Bajaj 等应用基于 Bezout 定理及其推广给出了解法, 参见 [Baj] 和 [B-I]. 而我们将采用完全不同的原理和方法来解决上述普遍性的问题. 下面我们将阐述该方法.

代数几何与微分几何的联系

注释 8.4.3 在实际应用中, 给出的仅是实曲线段 C_j 和实曲面片 S_j, 而所求的是一个实曲面片 S, 为此, 基域 $\mathbf{K}$ 取成实数域 $\mathbf{R}$. 我们将基于 5.1 节的 Whitney 的理论来处理实簇. 欧氏空间 $\mathbf{R}^n(X)$ 中具有实维数 d 的实簇是指有一实完备基底 $PS \in \mathbf{R}[X]$ 的簇, 它的复化 $\mathrm{Zero}_c(PS)$ 具有复维数 d. 于是, 实簇 $V = \mathrm{Zero}_{\mathbf{R}}(PS)$ 将有 Whitney 分解, 它的实流形分支的实维数将小于或等于 d, 而且, 那些实维数等于 d 的实流形分支实际上也存在.

定义 8.4.4 对实维 d 的簇 $V = \mathrm{Zero}_{\mathbf{R}}(PS) \subset \mathbf{R}^n(X)$, PS 是其实完备基. V 的 Whitney 分解中, 具有最高实维数 d 的流形分支称为实簇 V 的主分支.

定义 8.4.5 对于以 PS 为实完备基的, 实 d 维簇 $V = \mathrm{Zero}_{\mathbf{R}}(PS) \subset \mathbf{R}^n(X)$, 若 $\mathrm{Zero}(PS)$ 为不可约, 或者 $\mathrm{Zero}(PS)$ 在通常意义下是绝对不可约则称 V 不可约.

注释 8.4.6 在上述问题 SF 和下面的问题中, 我们所说的实曲线或曲面

是如定义 8.4.4 的，具有实维数 1 或 2 的实簇. 于是，它们实际上分别包含主分支或维数为 1 或 2 的某一片. 我们也假定实不可约即定义 8.4.5 中的不可约. 后面这一假设被假定成立，我们对此将不再明确说明.

注释 8.4.7　根据 Whitney 分解，一个实代数簇作为实点集构成实微分流形. 这样，我们所说的正则点，切平面，法平面，曲率等等就与普通微分几何中的一样了.

关于实簇的若干基本定理

定理 8.4.8　对于以 PS 为实完备基的不可约实簇 $V = \mathrm{Zero}_{\mathbf{R}}(PS) \subset \mathbf{R}^n(X)$, V 的主分支上的正则点是相应不可约簇 $\mathrm{Zero}(PS)$ 的单点.

证明　令 V 的实维数是 d, X_0 是 V 主分支上的正则点. 显然，对于通常意义下的 X^0 点处的切空间方程将定义如 §5.1 中描述的 $\mathrm{Zero}(PS)$ 上 X^0 点处的切空间. 因此，X^0 是 $\mathrm{Zero}(PS)$ 中一简单点. □

定理 8.4.9　对于以 PS 为实完备基的不可约实簇 $V = \mathrm{Zero}_{\mathbf{R}}(PS) \subset \mathbf{R}^n(X)$, 多项式 $P \in \mathbf{R}[X]$ 在整个代数簇 $\mathrm{Zero}(PS)$ 上为 0 当且仅当 P 在 V 的 Whitney 分解任一主分支中正则点上都为零.

证明　令 V 的实维是 d. 如 P 在整个簇 V 上不为 0, 那么 $\mathrm{Zero}(P)$ 与 $\mathrm{Zero}(PS)$ 将相交于一维数小于或等于 $d-1$ 的簇，其实部的实维数也将小于或等于 $d-1$. 因此，任一主分支中都将有点使 P 不为 0. 反方向显然. 定理得证. □

定理 8.4.10　令不可约簇 $V = \mathrm{Zero}_{\mathbf{R}}(PS)$ 如定理 8.4.8 和 8.4.9 所示. 那么，一实多项式在 V 的任一主分支的所有实正则点为 0 当且仅当此多项式在此簇之母点上为 0, 或者说，当且仅当此多项式对由此母点定义不可约升列的余式是 0.

证明　由前述定理及 3.6 节的定理可得到本定理. □

注释 8.4.11　定理 8.4.10 形成了解决问题 SF 的原理和方法的基础，见下面的定理 8.4.12~8.4.15.

解决问题 SF 的某些基本定理

令 $\mathbf{K} = \mathbf{R}$ 是实域，$n = 3$. 我们考虑一般实空间 $\mathbf{R}^3$ 中的实曲线及曲面. 我们用通常的 x, y, z 代替 x_1, x_2, x_3, 变量序为

$$x \prec y \prec z,$$

那么，定义 8.4.4, 8.4.5 中所说的 $\mathbf{R}^3$ 中的实不可约代数曲面将可由方程 $P = 0$ 定义，其中 P 是一实多项式，在 $\mathbf{C}$ 中不可约，且 $P = 0$ 具有实维数为 2 的实

轨迹. P 的主变元是 x, y 或 z. 如果 P 的主变元是 x, 那么 P 必是 x 的线性方程，此时曲面是平面 $x=$ 常数. 另一方面，$\mathbf{R}^3$ 中实不可约代数曲线，将由一不可约升列 $IRR=\{P_1,P_2\}$ 定义，其中 $P_1,P_2\in\mathbf{R}[x,y,z]$. P_1,P_2 的主变元是 x,y 或 x,z 或 y,z. 如果 P_1 的主变元是 x, P_1 关于 x 必然是线性的. 这样，曲线的实部完全位于平面 $x=$ 常数 中. 需要注意的是，一般情况下，由不可约升列 IRR 确定的实不可约曲线，即 $\mathrm{Var}[IRR]$ 的实部分与曲线 $\mathrm{Zero}(IRR)$ 的实部是不同的.

下面，C 是一不可约实代数曲线，也即由不可约升列 $IRR=\{P_1,P_2\}$ 确定的簇 $\mathrm{Var}[IRR]$ 的实部，其中 $P_1,P_2\in\mathbf{R}[\mathbf{x},\mathbf{y},\mathbf{z}]$, S, S' 是分别由 $P=0$ 及 $P'=0$ 定义的不可约代数曲面，$P,P'\in\mathbf{R}[x,y,z]$.

作为定理 8.4.10 的特殊情形，我们有以下定理.

定理 8.4.12 曲面 S 包含整条曲线 C 当且仅当

$$\mathrm{Remdr}(P/IRR)=0. \tag{8.4.85}$$

定理 8.4.13 假设 C 完全包含在 S 及 S' 中，而并未包含在 S 或 S' 的奇异轨迹中. 取 $P_x=\frac{\partial P}{\partial x}, P'_x=\frac{\partial P'}{\partial x}$ 等等，且建立下述多项式:

$$\left.\begin{aligned} D_1&=P_x*P'_y-P_y*P'_x,\\ D_2&=P_x*P'_z-P_z*P'_x,\\ D_3&=P_y*P'_z-P_z*P'_y,\end{aligned}\right\} \tag{8.4.86}$$

那么 S 及 S' 在 C 上所有的对 C,S,S' 都正则的点处沿 C 光滑拼接当且仅当

$$\mathrm{Remdr}(D_i/IRR)=0,\quad i=1,2,3. \tag{8.4.87}$$

证明 由微分几何知识我们有 S 及 S' 在 C 上所有正则点沿 C 光滑拼接当且仅当在这些点上 $D_i=0$, $i=1,2,3$. 而由定理 8.4.10 得知后者成立当且仅当 (8.4.87) 成立，因此定理成立. □

关于下面引理 8.4.14 的证明，我们可参考一些初等微分几何的著作，如 [Eish].

引理 8.4.14 对由 $P=0$ 定义的实不可约代数曲面，在正则点的曲率 κ 如下:

$$\kappa=\frac{V}{H^2}, \tag{8.4.88}$$

其中

$$H=\sqrt{P_x^2+P_y^2+P_z^2}, \tag{8.4.89}$$

$$V = Cyc(P_{xx} * P_{yy} * P_z^2 - 2 * Cyc(P_x * P_y * P_{xy} * P_{zz})) \\ +2 * Cyc(P_x * P_y * P_{xz} * P_{yz}) - Cyc(P_x^2 * P_{yz}^2). \tag{8.4.90}$$

(8.4.90) 中 Cyc 表示相应表达式关于变量 x, y, z 及 $P_x, P_{xx} = \frac{\partial^2 P}{\partial x^2}$ 的循环和，它们均取值于正则点.

定理 8.4.15　令 C, S, S' 满足定理 8.4.13 中的条件，如前所述. 那么，S, S' 在 C, S, S' 的正则点上具有相同曲率当且仅当

$$\text{Remdr}(H^2 * V' - H'^2 * V/IRR) = 0. \tag{8.4.91}$$

在 (8.4.91) 中 H' 及 V' 是关于 P' 的多项式，类似于 H 及 V 是关于 P 的多项式.

证明　对 C, S, S' 的正则点，我们有 $H \neq 0, H' \neq 0$. 因此由引理 8.4.14, 曲率 κ, κ' 将由 (8.4.88) 定义，它们相等当且仅当

$$H^2 * V' = H'^2 * V \tag{8.4.92}$$

对 C 上关于 C, S, S' 的所有正则点均成立. 由定理 8.4.10 知，后者与 (8.4.91) 等价，则定理得证. □

解决问题 SF 的方法

根据定理 8.4.12~8.4.15, 解决问题 SF 将转化成验证余式是否为 0, 而这可被进一步化简为多项式方程的求解，如下所示.

方法　对由 $P = 0$ 定义的幂次为 m 的不可约代数曲面，把 P 写成下述形式：

$$P = \sum_m u_{abc} * x^a * y^b * z^c, \tag{8.4.93}$$

其中的 $\sum_m$ 是在满足下述条件的三元组 (a, b, c) 上求和：

$$0 \leq a, \qquad 0 \leq b, \qquad 0 \leq c, \qquad a + b + c \leq m. \tag{8.4.94}$$

我们把满足 (8.4.94) 的所有 u_{abc} 的集合记成 U_m.

例如考虑 S 是否包含整条由不可约升列 IRR 定义的不可约代数曲线 C 的问题. 由定理 8.4.12, 其等价于考虑下述条件：

$$R = \text{Remdr}(P/IRR) = 0. \tag{8.4.95}$$

记 R 中变量 x,y,z 的不同幂次的系数构成的多项式集是 $US_0 \subset \mathbf{R}[U_m]$, 那么条件 (8.4.95) 等同于下述条件:

$$US_0 = 0. \tag{8.4.96}$$

为了满足问题 SF 中的条件 (1), 与 (8.4.96) 中 US_0 相似, 我们对每条曲线 C_i, C_j, C_k 构造多项式集 $US_{ai}, US_{aj}, US_{ak}$. 相似地, 对问题 SF 中的要求 (2), 由定理 8.4.13 可得多项式集 $US_{bi}, US_{bj}, US_{bk}$, 对问题 SF 中的要求 (3), 由定理 8.4.15 可得多项式集 US_{ck}, 它们的零点是将要证明的相应的条件. 注意到 $US_{ai}, US_{aj}, US_{ak}, US_{bj}, US_{bk}$ 关于 u 是线性的, 而 US_{ck} 关于 u 则一般非线性. 把上述所有多项式集合并成一多项式集 $US \subset R[U_m]$, 所有满足要求问题 SF 的解 S 由实零点集 $\mathrm{Zero}_{\mathbf{R}}(US)$ 给出.

<u>一些例子</u>

$\mathbf{R}^3$ 中一般三次曲面的形式为

$$\begin{aligned} f(x,y,z) = {} & u_{300} * z^3 + z^2(u_{210} * y + u_{201} * x + u_{200}) + z * (u_{120} * y^2 \\ & + u_{111} * y * x + u_{102} * x^2 + u_{110} * y + u_{101} * x + u_{100}) + u_{030} * y^3 \\ & + u_{021} * y^2 * x + u_{012} * y * x^2 + u_{003} * x^3 + u_{020} * y^2 \\ & + u_{011} * y * x + u_{002} * x^2 + u_{010} * y + u_{001} * x + u_{000} = 0, \end{aligned} \tag{8.4.97}$$

其中 u 都在实数域 $\mathbf{R}$ 上. 下面, 我们将通过几例表明如何采用我们的方法来确定一个三次曲面使其满足问题 SF 中的关于 (1), (2), (3) 的精确陈述中的某些要求.

例 8.4.16 在 $\mathbf{R}^3$ 中考虑以 x,y 轴为轴心线的两圆柱 CYL_1, CYL_2 及由平面截得的与此两轴分别垂直的两圆部分 C_1, C_2. 那么这些圆形部分将由升列 $AS_1 = \{C_{11}, C_{12}\}$ 及 $AS_2 = \{C_{21}, C_{22}\}$ 定义, 其中

$$C_{11} = x - d_1, \qquad C_{12} = z^2 + y^2 - r_1^2, \tag{8.4.98}$$

$$C_{21} = x - d_2, \qquad C_{22} = z^2 + x^2 - r_2^2, \tag{8.4.99}$$

而两圆柱则分别由 $C_{12} = 0, C_{22} = 0$ 定义. 很自然地, 我们假设 d_1, d_2, r_1, r_2 非 0, 且为正的. 现在我们确定一个三次曲面 (8.4.97), 使其包含圆 C_1, C_2 且沿圆与圆柱 CYL_1, CYL_2 光滑相接. 由我们的方法得 28 个方程, 用王定康的软件包 wsolve, 易得到这样的解存在当且仅当

$$r_1^2 + d_1^2 = r_2^2 + d_2^2, \tag{8.4.100}$$

在此情形，可能的三次曲面如下给出：

$$z^2*(y*d^2+x*d_1-d_2^2-d_1^2)+(y^3*d_2+x^3*d_1)+y*x*(y*d_1 \\ +x*d_2-2*d_2*d_1)-(y^2+x^2)*(d_2^2+d_1^2)+y*d_2*(d_1^2-r_1^2) \\ +x*d_1*(d_2^2-r_2^2)+(r_1^2+d_1^2)*(r_2^2+d_2^2)-2*d_1^2*d_2^2=0, \quad (8.4.101)$$

见图 8.8.

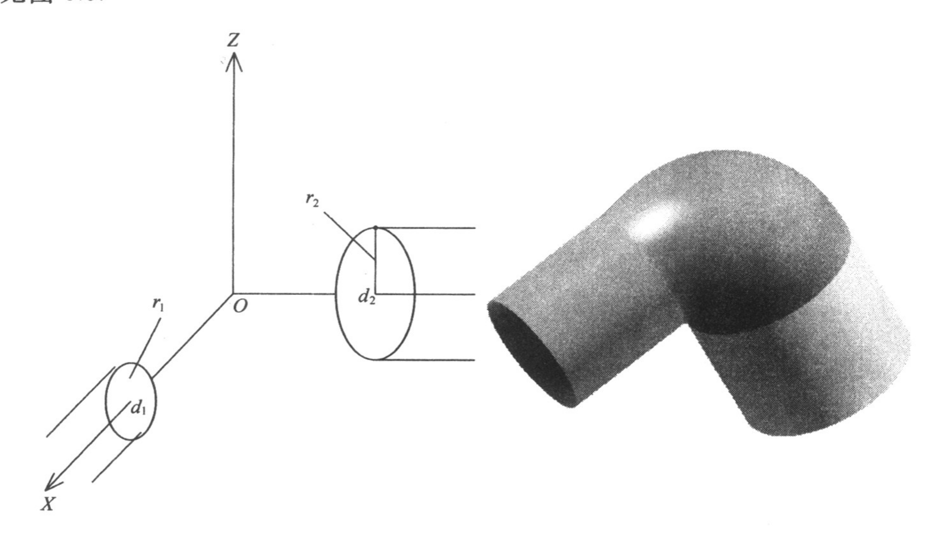


图 8.8　管道拼接

例 8.4.17　考虑圆 C_1, C_2 如例 8.4.16 所示，而第三个圆 C_3 以 z 轴为中心且垂直于此轴. 设升列 C_3 由 $\{C_{31}, C_{32}\}$ 定义，其中

$$C_{31}=y^2+x^2-r_3^2, \qquad C_{32}=z-d. \qquad (8.4.102)$$

如前所述，我们仍假设 d_i, r_i 为正. 软件包 wsolve 将给出此问题的可能的解的完全集. 另外，首先假设 d_i, r_i 完全任意，即是独立的参变量. 我们的方法表明包含三个圆弧的唯一的三次曲面是一个退化曲面，它是包含三个圆的三个平面. 假如 d_i, r_i 满足关系 (8.4.100) 而其他参数任意，那么除了由三个平面组成的退化曲面外，还仅有一族三次曲面，它们退化为包含圆 C_3 的平面及通过圆 C_1, C_2 的二次曲面，由如下方程给出 (其中，u_0 是参数):

$$(d_1*d_2+u_0)*(x^2+y^2+z^2)+(r_1^2+d_1^2)*(y*x-d_1*y-d_2*x) \\ -u_0*(r_1^2+d_1^2)=0. \qquad (8.4.103)$$

假设有关于 d_i, r_i 的下述关系式:

$$r_1^2 + d_1^2 = r_2^2 + d_2^2 = r_3^2 + d_3^2 = k^2. \tag{8.4.104}$$

而其他参数任意. 显然, 以原点为球心, 以 $|k|$ 为半径的球面将包含三圆 C_i. 除了任意平面, 有一族 ∞^3 退化的三次曲面包含三个圆. 然而, 我们的方法表明, 事实上, 共四族 $\infty, \infty^2, \infty^3, \infty^4$ 三次曲面包含三个圆. 包含球面和任意一平面的三次曲面其实仅是 ∞^4 族曲面的一个子集. 最后一族曲面依赖于参变量 $u_{100} : u_{002} : u_{010} : u_{001} : u_{000}$ 的比例. 设

$$\left.\begin{aligned} u_{111} = u_{110} = u_{101} = 0, \\ u_{201} = u_{003} = u_{021} = a, \\ u_{210} = u_{030} = u_{012} = b, \\ u_{300} = u_{120} = u_{102} = c, \\ u_{200} = u_{020} = u_{002} = -d, \end{aligned}\right\} \tag{8.4.105}$$

那么, 我们将得到作为 ∞^3 退化的三次曲面的子族, 其由一球面及平面 $a*x+b*y+c*z=d$ 构成. 对 ∞^4 族中而不在 ∞^3 中的三次曲面, 图 8.9 可给出一粗略的描述.

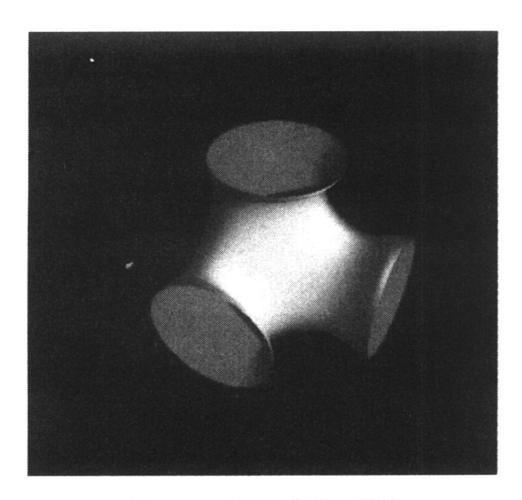


图 8.9 三圆柱曲面的拼接

我们的方法表明, 上述是包含三个圆的仅可能的三次曲面. 由于上面给出的非退化三次曲面族依赖于几个参数, 如果我们喜欢, 可采用我们的方法去决定满足进一步要求的曲面. 然而, 如果 $CYK_i (i = 1, 2, 3)$ 是以 x, y, z 轴为轴心

的圆柱，其分别以 $C_i(i=1,2,3)$ 为边，那么对于形式 (8.4.100) 不可能存在任一个三次曲面使其包含三圆且沿三圆与三圆柱光滑相接.

上述两例中的曲线如圆周，曲面如圆柱都容易参数化，随着这样的参数化，这些例子中的问题可采用其他方法给予解决，见 [Baj]. 然而，除了极少的有理情形，曲线曲面一般是不可进行参数化的，这对三次曲线与曲面依然如此，下例是不可用参数化方法来解决的.

例 8.4.18　令 $f_1(x,y,z), f_2(x,y,z)$ 如 (8.4.97) 中 $f(x,y,z)$, 其中 u 的系数分别由 a, b 所代替. 令 S_1, S_2 是分别由 $f_1=0, f_2=0$ 定义的不可约三次曲面. C_1, C_2 是分别由不可约升列 $IRR_1=\{y,g_1\}$, $IRR_2=\{y,g_2\}$ 定义的三次曲线，其中 $g_1=f_1(x,0,z)$, $g_2=f_2(x,y,0)$. 我们的问题是确定如 (8.4.97) 的三次曲面，它包含 C_1, C_2 且最终满足进一步要求. 现 C_1, C_2 交 x 轴于 $y=z=0$ 的点的 x 坐标由下述方程给出:

$$\left.\begin{aligned} a_{003}*x^3+a_{002}*x^2+a_{001}*x+a_{000}=0,\\ b_{003}*x^3+b_{002}*x^2+b_{001}*x+b_{000}=0. \end{aligned}\right\} \tag{8.4.106}$$

如存在包含 C_1, C_2 的三次曲面，相交点必须相同. 所以我们假设

$$a_{003}=b_{003},\qquad a_{002}=b_{002},\qquad a_{001}=b_{001},\qquad a_{000}=b_{000}. \tag{8.4.107}$$

为简化计算，我们假设相交点在 x 轴上均不为 0 或无穷大，于是

$$a_{000}=b_{000}\neq 0,\qquad a_{003}=b_{003}\neq 0. \tag{8.4.108}$$

我们进一步假设 z 轴不会渐近曲线 C_1, y 轴也不会渐近曲线 C_2, 这样

$$a_{300}\neq 0,\qquad b_{030}\neq 0. \tag{8.4.109}$$

在条件 (8.4.107)~(8.4.109) 下，应用软件包 wsolve, 我们的方法表明唯一包含两三次曲线的三次曲面将构成一族由下述方程定义的 ∞^4 三次曲面

$$\left.\begin{aligned}
&u_{000}*a_{300}-u_{300}*a_{000}=0, && u_{001}*a_{300}-u_{300}*a_{001}=0,\\
&u_{010}*a_{300}-u_{300}*b_{010}=0, && u_{002}*a_{300}-u_{300}*a_{002}=0,\\
&u_{011}*a_{300}-u_{300}*b_{011}=0, && u_{020}*a_{300}-u_{300}*b_{020}=0,\\
&u_{003}*a_{300}-u_{300}*a_{003}=0, && u_{012}*a_{300}-u_{300}*b_{012}=0,\\
&u_{021}*a_{300}-u_{300}*b_{021}=0, && u_{030}*a_{300}-u_{300}*b_{030}=0,\\
&u_{100}*a_{300}-u_{300}*a_{100}=0, && u_{101}*a_{300}-u_{300}*a_{101}=0,\\
&u_{102}*a_{300}-u_{300}*a_{102}=0, && u_{200}*a_{300}-u_{300}*a_{200}=0,\\
&u_{201}*a_{300}-u_{300}*a_{201}=0.
\end{aligned}\right\} \tag{8.4.110}$$

上述曲面族依赖于参数的比例

$$u_{110}:u_{111}:u_{120}:u_{210}:u_{300}, \tag{8.4.111}$$

因此，个数是 ∞^4 个. 如需要我们还可用我们的方法确定满足进一步要求的曲面子族.

§8.5 一些补充和扩展

求解四次方程

让我们考虑求解一个四次方程

$$f(z) \equiv z^4 + a * z^2 + b * z + c = 0,$$

L.Ferrari(+1522, +1565) 给出的经典求解方法需要一些技巧来把它化简为求解一个三次方程. 下面的方法，根据 [Lyon] 和 [Ku] 文章中的原始想法作了一定修改，看起来更加自然一些.

我们假定，像在 §4.5 中胡 - 王方法作因式分解一样， $f(z)$ 可以因式分解为

$$f(z) = (z^2 + x_1 * z + x_2) * (z^2 - x_1 * z + x_3),$$

其中 x_1, x_2, x_3 为待定系数. 比较两边不同的 z 的幂次，我们得到一个多项式集 $PS = \{P_1, P_2, P_3\}$, 以通过求解 $PS = 0$ 得出 x_1, x_2, x_3 :

$$\begin{aligned}
P_1 &= x_3 + x_2 - {x_1}^2 - a,\\
P_2 &= x_1 * (x_3 - x_2),\\
P_3 &= x_2 * x_3 - c.
\end{aligned}$$

我们容易得到

$$\text{Zero}(PS) = \text{Zero}(CS_1/x_1) + \text{Zero}(CS_2 + \{b\}),$$

其中 $CS_i = \{C_{i1}, C_{i2}, C_{i3}\}$, $i = 1, 2$, 且

$$\begin{aligned}
C_{11} &= x_1^6 + 2 * a * x_1^4 + (a^2 - 4 * c) * x_1^2 - b^2,\\
C_{12} &= 2 * x_1 * x_2 - x_1 * (x_1^2 + a) + b,\\
C_{13} &= x_3 + x_2 - x_1^2 - a,\\
C_{21} &= x_1,\\
C_{22} &= x_2^2 - a * x_2 + c,\\
C_{23} &= x_3 + x_2 - a.
\end{aligned}$$

因为 $b=0$, 所以我们讨论无意义的情形 CS_2. 而 $C_{11}=0$ 给我们一个关于 x_1^2 的三次方程，它起的作用类似于在 Ferrari 解法中的三次方程. 由于 $f(z)$ 的两个因子可以互换，由 x_1^2 表示成的三次方程是很自然的. 请注意这一简单的例子表明我们早在高中所学的简单原理和待定系数法，它们的作用是很强大的. 下面我们将给出一个用这种简单原理和待定系数法来处理更复杂的偏微分方程的问题.

金字塔问题

下面的问题，由张景中提出，由王定康解决，参见 [WDK2].

设 P-$ABCD$ 为一个顶点为 P 正方形底 $ABCD$ 的正则平方金字塔. 设一个平面 π 分别交五条边 AB, BC, CP, PD, PA 于五个点 E, F, G, H, I.

金字塔问题　判断能否选择平面 π 使得 $EFGHI$ 为一个正则五边形.

为了解决这个问题，我们引入一个坐标系，以底面正方形的中心 O 为原点，以 OC, OD 为正 x 轴和正 y 轴. 不失一般性，我们可以取 $|OC|$ 为单位长度，所以我们有

$$A=(-1,0,0),\quad B=(0,-1,0),\quad C=(1,0,0),\quad D=(0,1,0).$$

为使得 $EFGHI$ 为一个正则五边形，应该有 $GI\|EF\|AC$. 因此按照王定康的做法，我们可以这样取坐标，使得

$$\begin{aligned}&E=(-x_1,x_2,0),\quad F=(x_1,x_2,0),\quad G=(x_3,0,x_5),\\&I=(-x_3,0,x_5),\quad H=(0,x_6,x_7),\quad P=(0,0,x_9).\end{aligned}$$

由 $EFGHI$ 为一个正五边形，我们得到一个多项式集 $PS=\{P_1,\cdots,P_8\}$, 它有实零点对应于金字塔和平面 π 相交成正则五边形. 多项式 P_i 由下式给出：

$$\begin{aligned}
P_1&=x_2-x_1+1,\\
P_2&=x_9*(x_3-1)+x_5,\\
P_3&=x_9*(x_6-1)+x_7,\\
P_4&=x_7*x_2+x_5*(x_6-x_2),\\
P_5&=x_3^2+x_6^2+(x_7-x_5)^2-4*x_1^2,\\
P_6&=(x_3-x_1)^2+x_2^2+x_5^2-4*x_1^2,\\
P_7&=4*x_3^2-x_1^2-(x_6-x_2)^2-x_7^2,\\
P_8&=x_3^2-x_1*(x_3+x_1).
\end{aligned}$$

实零点集 $\mathrm{Zero}_R(PS)$ 可以用一般的特征列方法确定. 对于 $\mathrm{Zero}_R(PS)$ 的详细分析可以导出下面的定理：

定理 8.5.1 (金字塔定理) 对于一个正则正方金字塔 P-$ABCD$, 不致退化成 $P=O$, 容许切割出正五边形 $EFGHI$ 的充要条件是金字塔的高度 $|PO|$ 等于底面正方形对角线长度的一半. 在这种情况下, E,F,G,H,I 由下式完全决定 (其中 $\varepsilon=\pm1$)：

$$\begin{cases} x_1 = x_5 = x_6 = \dfrac{3+\varepsilon*\sqrt{5}}{2}, \\ \\ x_2 = -x_3 = -x_7 = \dfrac{1+\varepsilon*\sqrt{5}}{2}. \end{cases}$$

在公式中, $\varepsilon=-1$ 给出了切出正则五边形的情形, $\varepsilon=+1$ 给出了切出正则五星的情形. 参看图 8.10, 8.11.

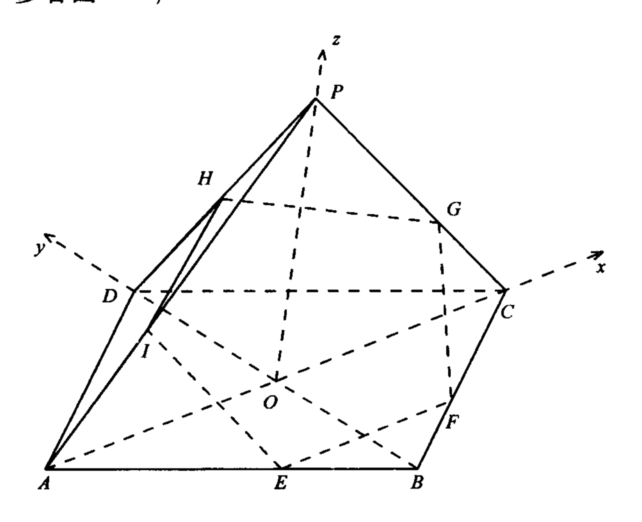


图 8.10 金字塔定理 a

几何构造的 Zassenhaus 问题

用直尺和圆规来构造一个给定三角形的角平分线, 这是很简单的问题. 但是反过来, 其逆问题是不简单的.

Zassenhaus 问题 判断能否仅用直尺和圆规根据已知的三条角平分线 (内角或外角) 几何地构造出一个三角形.

这个问题已被高小山和王定康完全解决, 并给出了否定的答案. 可参看 [WDK2]. 他们的方法如下.

设要构造的三角形的边为 $a,b,c(>0)$, 对应于已知的内角平分线 a_i,b_i,c_i (>0). 然后我们通过求解 $PS=0$, 用 a_i,b_i,c_i 来决定 a,b,c, 其中 $PS=$

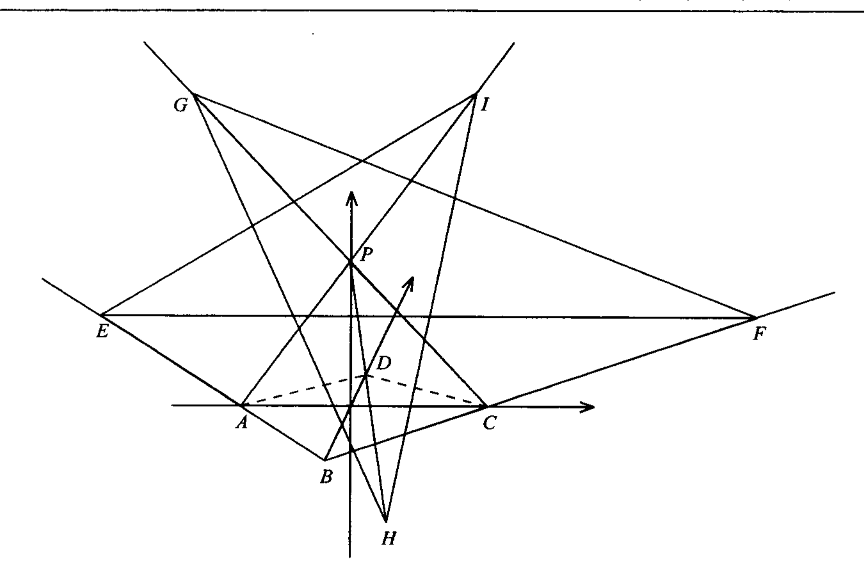


图 8.11 金字塔定理 b

$\{P_1, P_2, P_3\}$ 由下式所给出:

$$\begin{aligned}
P_1 &= (b+c)^2 * a_i^2 - b * c * (b+c-a) * (a+b+c),\\
P_2 &= (c+a)^2 * b_i^2 - c * a * (c+a-b) * (a+b+c),\\
P_3 &= (a+b)^2 * c_i^2 - a * b * (a+b-c) * (a+b+c).
\end{aligned}$$

考虑一般情形 a_i, b_i, c_i 为未定元，取变量序为 $a_i \prec b_i \prec c_i \prec a \prec b \prec c$. 可以求出 PS 的第一个特征多项式为一个 a^2 的 10 次不可约多项式，且有 331 项. 由于含 a 的多项式并不是 2 次的，由一般的理论可知，并不能从 a_i, b_i, c_i 仅用直尺和圆规来构造出所求的三角形. 问题解决. 对于三条角平分线中有一条或几条为外角平分线的情形，可以类似处理，并得到同样的结论.

一个 Erdös 问题

从 R. S. Boyer 跟周咸青和高小山的口头交流中，我们得知由 Erdös 提出的如下问题:

Erdös 的 10 点问题 在平面上给定 10 个点 $A_{ij}, 1 \le i < j \le 5$. 确定这样 5 个点 $B_i, i = 1, \cdots, 5$, 使得每一个点 A_{ij} 在连接点 B_i 和 B_j 的直线上.

很容易把这个问题转化为一个多项式求解问题. 在特征列方法的基础上应用一些 Clifford 代数的技巧，石赫和李洪波已经从本质上解决了这个问题的一般情形，其结果陈述如下 (参见他们的合作文章 [L-S]):

定理 8.5.2 对于一般的 A_{ij}, 最多存在 6 种可能的 5 点分布 B_i, 使得任一点 A_{ij} 在直线 B_iB_j 上.

计数几何中的 Poncelet 系论

让我们再考虑 (6.3) 节中的计数几何中的 EG 问题.

通过引入合适的坐标系，这样的问题可转化为求特定方程组的解的个数的问题. 然而，这种问题的结果通常可以以定理的形式表达. 于是这可以看作方程求解问题，也可以看作定理证明问题. 作为一个例子，我们考虑下面的问题:

Poncelet 系论 设 C 和 C' 为复射影平面中的两条给定二次曲线. 那么，如果存在一个三角形内接于两条曲线中的一条，比如 C, 且外切于另一条 C', 那么存在无穷多的这种三角形，内接于 C 外切于 C'.

我们可以把一个与上面定理有关的问题陈述为方程求解的形式:

问题 P 找出内接于一条二次曲线 C 外切于另一二次曲线 C' 的三角形的数目 N.

根据 Poncelet 定理我们有

(P1) 数目 N 或者为零，或者为无穷.

处理这种问题的一个现代代数几何方法是代数对应方法. 对于上面的问题 P 让我们考虑下面的代数对应. 在 C 上任取一个点 p_0. 过 p_0 作 C' 的切线相交 C 于另一点 p_1. 过 p_1 再作 C' 的切线相交 C 于另一点 p_2. 过 p_2 再作 C' 的切线相交于 C 于另一点 p_3. 那么 $p_0 \to p_3$ 建立了 C 到自身的代数对应关系. 这是一个 (2,2)- 对应，一般理论证明了存在 4 个或者无穷个不动点. 任一这样的不动点 $p_3 = p_0$ 将会给出一个三角形 $p_0p_1p_2$ 内接于 C 外切于 C' (见图 8.12). 然后我们就有

(P2) 数目 N 或者为 4 或者为无穷.

问题 P 的答案 (P1) 和 (P2) 之间的明显差异，是由于问题中几何概念的含义歧义性造成的. 因此，让我们考虑一般位置情形的两条二次曲线 C, C', 设 L_0 为一条公共切线切 C 于一点 p_1. 过 p_1 作 C' 的另一条切线 L_2, 交 C 于另一点 p_0. 从 p_0 开始，我们得到一个点列 $p_0, p_1, p_2(= p_1)$, $p_3(= p_0)$, 且上面的点 p_0 是代数对应 $p_0 \to p_3$ 的一个不动点. 这个不动点 p_0 产生一个 退化三角形$p_0p_1p_2$, 且被看作内接于 C 外切于 C' 的三角形而计算在内. 由于 C 和 C' 有四条公切线，也就有四个这样的退化三角形，这就解释了答案 (P2) 中的数字 4 的含义. 另一方面，这种退化三角形并不能看作对于 Poncelet 系论的问题 P

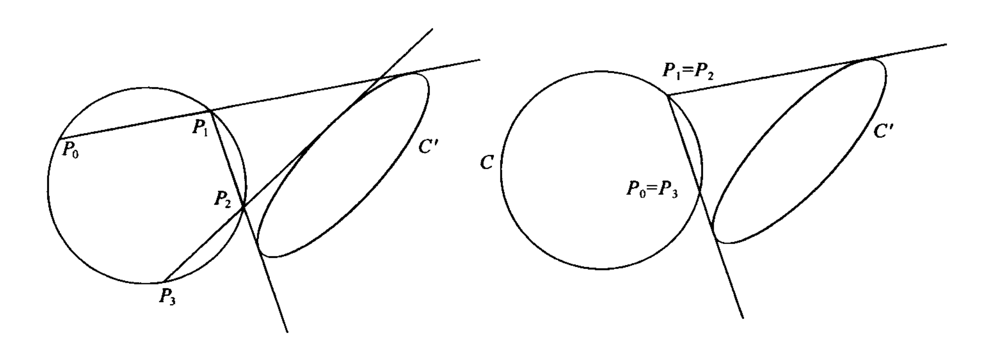


图 8.12 问题 P 的答案 (P1)　　图 8.13 问题 P 的答案 (P2)

的解，也解释了答案 (P1) 中的数字 0 的含义．参见图 8.13.

为了矫正这个问题，我们首先应该对于涉及的几何概念给出精确的定义．于是有：

对于一个三角形，我们称三个点 p_0,p_1,p_2 为 顶点，三条直线 L_0,L_1,L_2 为边，并使得 p_0 在直线 L_1 和 L_2 上，p_1 在直线 L_0 和 L_2 上，p_2 在直线 L_0 和 L_1 上．也就是说，我们需要 L_0 通过 p_1 和 p_2，L_1 通过 p_0 和 p_2，L_2 通过 p_0 和 p_1．注意到点 p_0,p_1,p_2 并没有要求互异，类似地，直线 L_0,L_1,L_2 也未必不同．于是，我们允许退化三角形．点 - 边对 $(p_0,L_0),(p_1,L_1),(p_2,L_2)$ 称为 对应对.

上面的三角形称为内接于曲线 C，如果直线 L_0 交曲线 C 于点对 p_1,p_2(不管重合与否)，且类似地，直线 L_1 交曲线 C 于点对 p_0,p_2，直线 L_2 交曲线 C 于点对 p_0,p_1.

上面的三角形称为外切于曲线 C'，如果直线对 L_1,L_2(不管重合与否) 为曲线 C' 的过点 p_0 的切线，且类似地，直线对 L_0,L_2 为曲线 C' 的过点 p_1 的切线，直线对 L_0,L_1 为曲线 C' 的过点 p_2 的切线.

在上面的例子中，我们记通过点 $p_2(=p_1)$ 与 C' 相切的异于 L_0 的另一条直线为 L_1，那么 L_1 和 L_2 重合，且三点 (p_0,p_1,p_2) 和三边 (L_0,L_1,L_2) 就形成了上面意义下的三角形．通过点 p_0 相切于 C' 的切线有两条，不是 L_1 和 L_2，而是 L_1(或 L_2) 和另一条 C' 的切线．所以这个三角形内接于曲线 C，但在上面的意义下并不外切于曲线 C'．这就说明了代数对应方法虽然是一个极端强大的方法，但有时也会对几何的问题给出一些额外的解.

现在我们用前面章节中的方法给出问题 P 的解.

由于仅对于 C' 作切线，首先我们把 C 看作一条点二次曲线，把 C' 看作一条线曲线．不丢失几何意义下，我们假定 C 不会退化为一对直线，C' 不会退

化为一对点. 又假定 C 和 C' 不是互为对偶. 在上面的假定下, 总能找到一个基本三角形, 由三个相异顶点 a_0, a_1, a_2, 三条相异边 S_0, S_1, S_2 构成, 且 (a_i, S_i) 为对应对, 使得 S_0, S_2 组成过 a_1 曲线 C' 的两条切线, S_0, S_1 组成过 a_2 曲线 C' 的两条切线, a_1 和 a_2 组成 S_0 交 C 的两个点.

设相对于上面的基本三角形任意标度的齐次坐标为 $(z_1 : z_2 : z_2)$, 且它的对偶直线坐标为 $(u_1 : u_2 : u_3)'$. 那么点二次曲线 C 和线二次曲线 C' 可以用点 - 线坐标的方程表示如下:

$$
\begin{aligned}
C\ &: x_{10} * z_1^2 + x_{11} * z_2 * z_3 + x_{12} * z_1 * z_3 + x_{13} * z_1 * z_2 = 0, \\
C'\ &: x_{21} * u_2 * u_3 + x_2 2 * u_1 * u_3 + x_{23} * u_1 * u_2 = 0.
\end{aligned}
$$

我们称有三点 (p_0, p_1, p_2) 、三边 (L_0, L_1, L_2) 和对应对 $(p_0, L_0), (p_1, L_1), (p_2, L_2)$ 的三角形为相对于二次曲线对 (C, C') 的一个 Poncelet三角形, 如果 L_0 交 C 于点 p_1 和 p_2, 过点 p_0 曲线 C' 的切线为 L_1 和 L_2, 等等. 我们注意到, 一个基本三角形成为 Poncelet 三角形的充分必要条件是 a_0 在 C 上或者 $x_{10} = 0$.

现在我们的问题是决定相对于 C, C' 的这种 Poncelet 三角形的个数 N.

假定存在一个如上定义的相对于 C, C' 的 Poncelet 三角形, 顶点 (p_0, p_1, p_2)、三边 (L_0, L_1, L_2), 然后通过引入相当于基本三角形的 p_i 的点坐标和 L_i 的线坐标, 我们得到一个多项式集 PS, 包含有 24 个多项式 P_i, P_i 中有 18 个未知比率和 7 个已知参数 $x_{10}, x_{1i}, x_{2i}, i = 1, 2, 3$. 18 个未知比率的数目少于 24 个实际方程 $P_i = 0$ 的数目, 这意味着 24 个方程不是无关的. 这对我们的一般方法无影响.

这个问题于是化简为决定 $\mathrm{Zero}_C(PS)$ 的问题, 如果其存在, 将对应于存在的 Poncelet 三角形. 这就引入了对 PS 和 $\mathrm{Zero}_C(PS)$ 的判定. 其中的细节我们可以参考文章 [WWT29], 下面仅以定理的形式给出最终结果.

定理 8.5.3 (Poncelet) 相对于互不对偶且非退化的一条点二次曲线和一条线二次曲线的 Poncelet 三角形的数目为零或者无穷, 除非曲线处于某些特殊的相对位置上.

作为这种特殊相对位置的一个例子, 我们可以这样得到: 任取一非退化点二次曲线 C, 在其上任取两个不同的点 p_0, p_1. 取 $p_2 = p_1$, 记直线 p_0p_1, p_0p_2 为 L_2 和 L_1, 这实际上是同一条直线. 设 L_0 为在 p_1 点处 C 的切线. 设 C' 为任一非退化的且包含 L_0 和 $L_1 = L_2$ 的线二次曲线, 且切 $L_1 = L_2$ 于点 p_0. 那么 C, C' 就组成了一对特殊相对位置的二次曲线. 在这种情形下, 我们看到三元组 (p_0, p_1, p_2) 和 (L_0, L_1, L_2) 组成相对于 C, C' 的一个 Poncelet 三角形. 只要

C' 作一般地选择，所以 Poncelet 三角形的个数既不是 0，也不是无穷，参看图 8.14. 上面的内容基本上是 [WWT29] 中相关段落的复制.

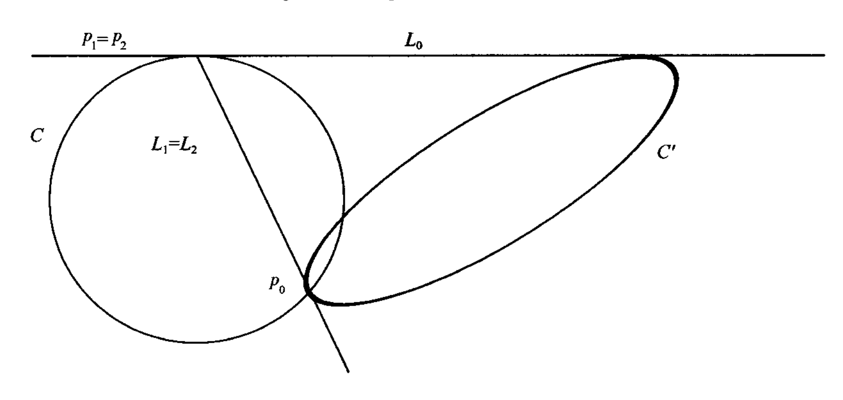


图 8.14 Poncelet 定理

有限几何中的定理证明

在这本书中我们限定于讨论基域 K 为特征零的情形. 然而在理论和应用中对于有限特征也很感兴趣，例如编码理论，密码学，区域设计，等等. 林东岱和刘卓军已经研究过有限特征的情形，并把他们的方法应用到有限几何的几何定理证明中. 参看他们的合作文章 [L-L].

让我们考虑有限射影几何 $PG(2,\mathbf{F}_q)$，其中 $\mathbf{F}_q$ 为由 $q=p^m$ 个元素组成的有限域，p 为一个素数. 良序原理和几何定理证明的方法可以用类似于特征零情形中的方式建立起来，仅仅计算是在整数上而不是在有理数上进行，应注意整数因子可被有限特征 p 整除的情形.

在特征 2 的平面 Fano 几何中，一个著名的例子就是存在互不相同的 7 个点 A,B,C,D,E,F,G，对于七个三元组 $ADC,AGE,AGC,AFB,CGF,CEB,DEF$ 中的任一组都是在同一条直线上，而 7 点中任意四点都不在同一直线上. 很明显，这种情形在特征零的情况下是不会出现的. 林和刘也发现了一些在有限特征下特有的有趣结果. 进一步地，他们的结果显示了在 p 为偶数和奇数情形的明显区别. 参见他们的定理如下：

定理 8.5.4 对于 $p=2$ 的情形，在 $PG(2,\mathbf{F}_q)$ 中的一个完全四边形的对角点永远是共线的.

定理 8.5.5 在一条曲线上没有三个不同点可以是共线的.

定理 8.5.6 如果 p 为奇数，那么一条曲线的三条不同切线不可能是相交于一点的.

定理 8.5.7 如果 p 为偶数，那么一条曲线的所有切线是相交于同一点的.

代数曲线的亏格

R. MacPherson, J. Mather, J. P. Brasselet, Mad. Schwartz 等人给出了具有任意奇点的射影 (不可约) 代数簇的 Chern 示性类的几种定义. 在这些定义中，由作者 (下面引用作吴) 给出的定义具有可计算的特性，参看 §5.3. 刘先仿 (参看 [LXF1,2]) 给出了这些定义的对比，并证明了如下定理:

定理 8.5.8 吴给出的 Chern 示性类定义与 Mather 给出的定义一致，但与 MacPherson 给出的定义不同.

另一方面，吴给出了对于任意不可约簇的 Chern 数的可计算方式的定义，而其他人甚至没有给出 Chern 数的定义. 利用吴的可计算定义，刘给出了计算一个不管是否平坦的复射影不可约曲线的亏格的整洁的显示公式，定理如下:

定理 8.5.9 设 C 为一条复代数不可约曲线，奇点 p_i 的重数为 m_i. 设 $\pi: \tilde{C} \to C$ 为 C 的一个光滑分解，那么 C 的亏格 $g(C)$ 可由下式给出:

$$g(C) = 1 - \frac{1}{2} * [C_{W1}(C) + \sum_i (|\pi^{-1}(p_i)| - m_i)],$$

其中，$C_{W1}(C)$ 为吴意义下的 C 的第一 Chern 数，其计算公式为 $C_{W1}(C) = 2 * Ord(C) - \text{Rank}(C)$; $|\pi^{-1}(p_i)|$ 为 C 在点 p 处的局部解析分支的个数.

注意到求一条奇异曲线的亏格公式只有在平坦的情形是已知的，其形式在复杂的情形下是难以计算的. 另外， J. Y. Zhou 也研究过吴的定义并跟其他的定义做了比较，参见文章 [Zhou].

非线性发展方程的孤波解

非线性发展 PDE(偏微分方程) 在数学物理中非常流行，寻找特定形式的精确解对于一些高科技应用具有非常重要的意义. 寻找这种精确解并没有一般的方法，通常需要用到一些复杂的技巧. 然而李志斌和他的合作者们设计了一种方法可应用到一类很广泛的非线性发展 PDE 中. 这种方法通过化简为多项式方程求解问题，得到许多的孤波解，从而得到特定形式的所有解. 这种方法概述如下.

李注意到大多数非线性发展 PDE 的孤波解可以写成双曲正切函数的形式. 于是考虑一个关于未知波函数 $u(x,t)$ 的 PDE, x 为位置变量, t 为时间变量. 一个行波解可以是形如 $u(x,t) = v(z)$, 其中 $z = k * x - \omega * t,k$ 为波数,

$c = \frac{\omega}{k}$ 为波速. 进一步引入变量 $y = \tanh(z)$, 使得 $v(z) = w(z)$ 对于某个函数 w. 问题于是化简为从用 w 表达的特定形式的所有波解中提取孤波解的问题, 这可以用一般的方法来解决. 我们于是考虑如下的行波解 w:

$$w = \sum_i a_i * y_i,$$

其中求和从 $i = 0$ 到 $i = m$, a_i 为含 k 的系数函数, ω 待定. 现在用 $u(x,t) = w(y)$ 代入给定的 PDE, 按照待定系数法, y 的各个幂次项的系数为零. 我们于是可以求出 m 的值, 得到一个含有系数 a_i 的多项式集, 这就给出了用上面 w 形式表达的给定 PDE 的所有可能解.

作为一个简单例子, 我们来考虑经典的 KdV 方程:

$$u_t + u * u_x + p * u_{xxx} = 0.$$

为了找到上面形式的所有解 w, 像上面一样, 我们令 $z = k*x - w*t$, $y = \tanh(x)$, $w = \sum_i a_i * y_i$. 我们容易得到 $m = 2$ 和一个多项式集 $PS = \{P_1, \cdots, P_6\}$ 如下:

$$\begin{aligned}
P_1 &= (2 * k^3 * p + \omega - k * a_0) * a_1,\\
P_2 &= k * a_1^2 + 16 * k^3 * p * a_2 + 2 * \omega * a_2 - 2 * k * a_0 * a_2,\\
P_3 &= (8 * k^3 * p + \omega - k * a_0 + 3 * k * a_2) * a_1,\\
P_4 &= -k * a_1^2 + 40 * k^3 * p * a_2 + 2 * \omega * a_2 - 2 * k * a_0 * a_2 + 2 * k * a_2^2,\\
P_5 &= -3 * k * a_1 * (2 * k^2 * p + a_2),\\
P_6 &= -2 * k * a_2 * (12 * k^3 * p + a_2).
\end{aligned}$$

当 $a_2 \neq 0$ 时, PS 的特征列为 $CS = \{C_1, C_2, C_3\}$,

$$\begin{aligned}
C_1 &= k * a_0 - 8 * k^3 - \omega,\\
C_2 &= a_1,\\
C_3 &= a_2 + 12 * k^2 * p.
\end{aligned}$$

由特征列 CS 我们可以得到无穷多解, 由 k, ω(也包括 p) 作参数, 表达如下:

$$u(x,t) = \frac{8 * k^3 * p + w}{k} - 12 * k^2 * p * \tanh^2(k * x - \omega * t).$$

特别地, 令 $\omega = 4 * k^3 * p$ 代入, 我们得到经典的孤子解:

$$u(x,t) = 12 * k^2 * p * \mathrm{sech}^2(k * (x - 4 * k^2 * p * t)).$$

可见已知的孤子解是我们用几乎平凡的方式得到的无穷多可能解中的一组特殊的解. 要知道更多的细节、例子和扩展请参看文章 [LZB], [ZSQ] 和 [Li-Ch].

化学反应平衡问题

许多来自于化学工程的非线性规划问题可导出非线性多项式方程求解问题. 在这些化学工程问题中化学反应平衡问题被认为是最困难的问题, 应受特别的注意. 我们考虑 n 种化学物质的混和物, 平衡时第 i 种物质为 x_i 摩尔. 令 $x_0=\sum_i x_i$. 那么这种混和物在温度 T 和压强 P 的条件下的自由能量为

$$F(X)=\sum_i x_i*\left(c_i+\ln\frac{x_i}{x_0}\right).$$

上式中 $c_i=\frac{F_i}{R*T}+\ln P$ 为已知常数, $\frac{F_i}{R*T}$ 为第 i 种物质的 Gibbs 自由能量. 混和物到达平衡时, 各个值 $x_i>0$ 应使得 $F(X)$ 达到最小值, 并遵守质量守恒方程:

$$\sum_i a_{ij}*x_i=b_j,\qquad j=1,\cdots,m.$$

在这些方程中, m 为不同原子的种类的数目, a_{ij} 为第 i 种物质的原子中含有元素 j 的原子数, b_j 为混和物在开始时含有第 j 种元素原子的重量的总数. 现在令

$$h_0=x_0-\sum_i x_i,$$

$$h_j=\sum_i a_{ij}*x_i-b_j,\qquad j=1,\cdots,m.$$

不失一般性, 我们假定 x_i 的多项式 h_j 的系数矩阵的秩恰好为 m, 否则开始时就可舍弃冗余的部分. 我们于是可以形成 Lagrange 多项式, λ_j 为 Lagrange 乘子:

$$L=F(X)+\lambda_0*h_0+\sum_j\lambda_j*h_j.$$

又令

$$e_j=\exp(-c_i),\qquad i=1,\cdots,n,$$
$$y_j=\exp(-\lambda_j),\qquad j=1,\cdots,m,$$

那么, 由 $\frac{\partial L}{\partial x_i}=0, i=0,1,\cdots,n$, 得到 $\lambda_0=1$, 且

$$P_i\equiv e_i*x_0*\Pi_j(y_j^{a_{ij}})-x_i=0,\qquad i=1,\cdots,n.$$

对于 Lagrange 多项式集我们有 $\mathrm{Zero}_R(LAG)=\mathrm{Zero}_R(PS)$, 其中 $PS=\{P_i,h_0,h_j\}$ 是一个 x_0,x_i,y_j 的多项式集. 由秩的假设, 对于 Jacobi 多项式集 JAC 有

$\mathrm{Zero}_R(JAC) = 0$, 用 §5.5 中的方法可决定 $D\mathrm{Zero}_R(PS)$ 的问题，其中 D 为由 $x_0 > 0$, $x_i > 0$, $y_j > 0$ 所定义的开域，$e_i > 0$ 看作已知参数.

作为一个具体例子，我们考虑这样一个反应平衡问题，在已知的温度 T 和压强 P 下，$\frac{1}{2}$ 摩尔的联氨 (hydrazine)N_2H_4 和 $\frac{1}{2}$ 摩尔的氧气 O_2 组成的 stoichiometric 混和物的燃烧问题. 平衡时的混和物含有 10 种物质:

$$\mathrm{H}, \mathrm{H_2}, \mathrm{H_2O}, \mathrm{N}, \mathrm{N_2}, \mathrm{NH}, \mathrm{NO}, \mathrm{O}, \mathrm{O_2}, \mathrm{OH}.$$

所以 $n = 10, m = 3$. 这个问题已经在很多文献中用多种方法研究过. 为了应用在 (5.5) 节中发展的方法，我们首先引入变量的序:

$$y_1 \prec y_2 \prec y_3 \prec x_1 \prec \cdots \prec x_{10} \prec x_0.$$

我们的方法然后导出一个多项式集，由此得出具有如下索引集 (index-sets) 的特征列 CS:

$$[1118\ \ y_1\ \ 12], [210\ \ y_2\ \ 1], [8\ \ y_3\ \ 1], [6\ \ x_1\ \ 1], \cdots.$$

因为在过程中去掉的初式和因子在通常情形下是非零的，$D\mathrm{Zero}_R(CS)$ 提供了所有的可能解，从中可以决定具有最低自由能量 $F(X)$ 的解. 这可跟通常的数值方法作一下对比，数值方法通常对于优化问题仅提供了一个可能的解，具有局部极值但不一定是全局最优的解. 细节可参看文章 [WWT15].

<u>微分情形下的推广</u>

特征列的理论和方法已经扩展到微分的情形，类似地可引入相关概念，如：微分多项式，微分多项式集，微分基本列，微分特征列，等等. 参看文章 [WWT33]. 注意我们的理论很大程度上依赖于 Ritt 的两本经典著作 [Ritt1,2] 和 Riquier 以及 Janet 的一些早期工作. 在单个独立变量情形下的理论实际上平行于通常多项式的情形，并已经应用到微分几何中曲线理论的定理证明中. 特别地我们仔细地研究过 Bertrand 曲线对 (pair) 在通常空间和仿射空间中的定理，参看文章 [WWT31,34]. 作为在 §8.1 中多项式情形下未知关系自动推导一般方法的一个推论，可以从 Kepler 定律自动推导出 Newton 定律. 这也应用到天体力学中的 Kepler 方程的求解. 另一方面，曲面和高维微分流形的定理证明也仅能片断地涉及. 在这个意义下，除了文章 [WWT34] 外，我们可以参看周咸青，高小山，李子明的相关文章，特别地推荐李洪波的文章 [LHB1,2].

天体力学中的 Kepler 方程

下面基本上是文章[WWT34]中一些相关段落的复制,也可参看文章 [W-W].

在天体力学中, Kepler 方程在天文计算中扮演了重要角色. 作为说明我们的一般方法的例子, 我们证实如何用完全不同于通常方法的方式来求解 Kepler 方程.

为了这个目的, 我们考虑一个行星 P 绕着恒星 S 作椭圆轨道运行, 偏心率为 e, 周期为 T. 设 t 为从近日点 II 开始计时所逝去的时间. 要确定角度 E, 是由朝向近日点的主轴和从椭圆轨道中心出发到 Q 点的半径向量所张成的角, 其中 Q 点为外切圆上与行星 P 在主轴上的投影为同一点 R 的一点. 参看图 8.15.

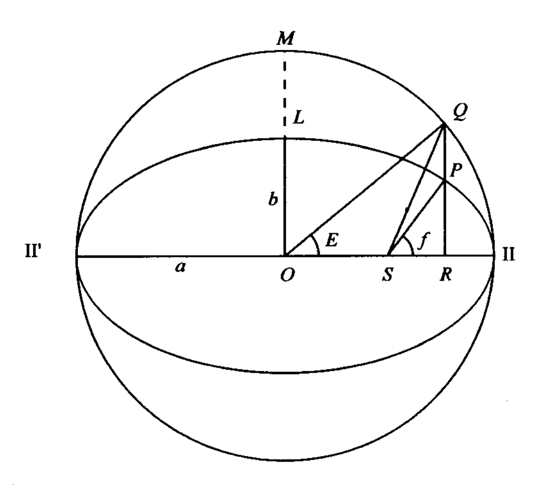


图 8.15 天体力学中的 Kepler 方程

Kepler 方程允许我们决定 E, 于是得到如下形式:

$$E - e * \sin E = M,$$

其中 $M = \frac{2*\pi*t}{T}$. 这个方程通常用数值或者图形方法来求解. 由 E 的用 e 展开的 Lagrange 级数也可以给出一个解, 级数中的系数为 $\sin M$ 相对于 M 的幂次的导数的形式, 也就是说:

$$E = M + \sum_n \frac{e^n}{n!} * \frac{d^{n-1}(\sin^n M)}{dM^{n-1}},$$

其中求和从 $n = 1$ 到 ∞.

Lagrange 级数的导数是相当复杂的，且级数仅当 e 充分小时才收敛，亦即 $e < 0.6627\cdots$. 我们现在应该给出一个简单的部件，把方程转换成可以用我们的一般方法以 M 的收敛级数的形式来决定 E 的形式，如类似 $\sin E$ 这样的 E 的简单函数.

这个方法的根本原理是非常简单的. 让我们把 $\sin E$ 看作一个独立的未知函数，令

$$F = \sin E.$$

正弦函数跟数学中出现的大多数超越函数一样，满足一个微分方程. 这个微分方程和原先的 Kepler 方程一起，组成了关于独立变元 M 的一个微分多项式集 $DPS = \{E, F\}$. 应用我们的一般方法，可以从 E 或 F 中得到方程组，进一步求解为 M 的级数的形式.

这个计算是非常简单的，步骤如下. 把 E 和 F 看作 M 的函数，用撇号 (′, prime) 表示相对于 M 的导数，我们从 $F = \sin E$ 得到

$$\begin{aligned} F' &= \cos E * E', \\ F'' &= -\sin E * E'^2 + \cos E * E''. \end{aligned}$$

我们用方程 F 和 F' 来去掉 Kepler 方程和方程 F'' 中的 $\sin E, \cos E$, 得到方程 $DP_1 = 0, DP_2 = 0$, 其中 DP_1, DP_2 如下式:

$$\begin{aligned} DP_1 &= E - e * F - M, \\ DP_2 &= E' * F'' - F' * E'' + F * E'^3. \end{aligned}$$

对于微分多项式集 $DPS = \{DP_1, DP_2\}$ 应用我们的一般方法，就可以得到需要的 E 或 F 的方程组.

例如，为了求解 E, 我们取定序为 $E \prec F$. 为了构造 DPS 相对于这个序的微分特征列 (d-char-set), 我们可构造 DP_2 相对于 DP_1 的微分余式 (d-remainder), 于是得到一个微分多项式:

$$DC_1 = E'' + (E - M) * E'^3.$$

上式和 $DC_2 = DP_1$ 合在一起组成了 DPS 相对于如上序的微分特征列. 方程 $DC_1 = 0$, 或

$$E'' + (E - M) * E'^3 = 0$$

于是成为关于 M 的方程，正如所求. E 和 E' 在 $M=0$ 处的初值易知为

$$E(0)=0, \quad E'(0)=\frac{1}{1-e}.$$

我们于是得到级数形式：

$$E=\frac{1}{1-e}*M-\frac{e}{(1-e)^4}*\frac{M^3}{3!}+\cdots.$$

由微分方程的一般理论知，上式在 $M=0$ 的邻域内收敛. 实际上可以证明，上式在所有 M 的取值上都收敛.

如果对于决定 $F=\sin E$ 感兴趣，我们可以取定序为 $F\prec E$ 以取代 $E\prec F$. 跟上面过程一样，构造 DP_2 相对于 DP_1 的微分余式，但现在是相对于新的次序. 我们得到一个如下微分多项式：

$$DC_1'=F''+F*(e*F'+1)^3.$$

上式和 $DC_2'=DP_1$ 合在一起组成了 DPS 相对于当前序的微分特征列. 方程 $DC_1'=0$, 亦即

$$F''+F*(e*F'+1)^3=0$$

给出了关于 M 的方程 $F=\sin E$. 在 $M=0$ 处的初值易知为

$$F(0)=0, \quad F'(0)=\frac{1}{1-e}.$$

我们于是得到所求的 $\sin E$ 的级数形式：

$$\sin E=\frac{1}{1-e}*M-\frac{1}{(1-e)^4}*\frac{M^3}{3!}+\cdots.$$

也可以证明，这个级数在所有 M 的取值上都收敛.

上面的方法是非常一般的，可以用来求出用M的项表达的 $\cos E$, 恒星 - 行星半径向量，近点角 (anomaly), 等等. 它也可以应用到抛物型和双曲型的轨道情形.

从 Kepler 定律自动推导出 Newton 定律

像在 Kepler 方程一节一样，下面基本上是文章 [WWT34] 中一些相关段落的复制. 也可参看文章 [WWT32].

Newton 从 Kepler 定律推导出了万有引力定律，这是一个重要的历史事件. 作者 1986 年在 Argonne 国家实验室访问期间，由 J. R. Gabriel 教授告知

用力学方式从 Kepler 定律推导出 Newton 万有引力定律的重要意义. Gabriel 教授已经成功地应用自己的自动推理方法来得到这个结果, 参看文章 [GAB]. 作为描述我们的一般方法的一个深入的例子, 我们下面说明一下怎么用我们的方法来处理这类问题.

为了达到这个目的, 我们首先把 Kepler 定律 (K) 和 Newton 定律 (N) 公式化地描述成如下形式:

(K_1) 行星以恒星为焦点作椭圆轨道运动.

(K_2) 从恒星到行星的向量在相等的时间里扫过相等的面积.

(K_3) 行星运动周期的平方与椭圆轨道主轴长度的立方成正比.

(N_1) 行星的加速度与行星到恒星的距离的平方成反比.

(N_2) 行星加速度向量的正向指向恒星.

(N_3) 平方反比律 (N_1) 中的比例因子与具体的行星无关.

为了机械化地推导, 甚至从 Kepler 定律自动发现 Newton 定律, 我们首先取一个坐标系, 把各个定律转化成方程的形式如下.

我们取直角坐标系 (x, y), 以恒星为原点, 以椭圆轨道的主轴为 X 轴. 设 r 为从恒星到行星的半径向量, 那么轨道就是如下形式的方程:

$$r = p + e * x. \tag{8.5.112}$$

Kepler 定律 (K_1) 于是对应于方程 (8.5.112), 也即是 (8.5.113)~(8.5.115) 合到一起:

$$r^2 = x^2 + y^2, \tag{8.5.113}$$

$$p = \text{const} \qquad \text{或} \qquad p' = 0, \tag{8.5.114}$$

$$e = \text{const} \qquad \text{或} \qquad e' = 0, \tag{8.5.115}$$

其中撇号 (′) 表示相对于时间 t 的导数. 类似地, Kepler 定律 (K_2) 对应于方程

$$x * y' - y * x' = h, \tag{8.5.116}$$

$$h' = 0. \tag{8.5.117}$$

对于 (K_3), 设 T 为行星沿椭圆轨道绕恒星运行一次的周期, $2 * a, 2 * b$ 为椭圆轨道的长轴长和短轴长. 那么 Kepler 定律 (K_3) 意味着 $\frac{T^2}{a^3}$ 是一个与行星无关的通用常数, 尽管可能与恒星有关. 现在, 根据 h 的意义, 我们有

$$h * T = 2 * \pi * a * b.$$

由于 $\frac{b^2}{a}=p$, 我们有

$$\frac{T^2}{a^3}=4*\pi^2*\frac{p}{h^2}.$$

由上式易知

$$c=\frac{p}{h^2} \tag{8.5.118}$$

也是一个与行星无关的通用常数，且 $c'=0$. 另一方面，记加速度为 A, Newton 定律 (N_1) 和 (N_2) 对应于如下的方程集:

$$A^2=x''^2+y''^2, \tag{8.5.119}$$

$r^2*A=\text{const}$, 或者由于 $r\neq 0$,

$$2*r'*A+r'*A'=0, \tag{8.5.120}$$

$$x*y''=y*x''. \tag{8.5.121}$$

对于 Newton 定律 (N_3), 常数 r^2*A 类似于 (N_1) 中的断言，是一个通用常数，因此可能存在 c 把这些常数联系起来，我们试图找出它来.

由于 Newton 定律 (N_2) 对应于 (8.5.121) 可直接从 Kepler 定律 (K_2) 对应于 (8.5.116) 和 (8.5.117) 而得出，我们下面仅考虑定律 (N_1) 和 (N_3).

为达到这个目的，我们首先引入未定元 x_{ij} 替换各个函数如下:

$$(r,A,c,p,e,x,y,h)=(x_{11},x_{12},x_{15},x_{21},x_{22},x_{31},x_{32},x_{51}).$$

各个函数安排得使 r,A,c 在前面以发现它们之间可能的关系. 通过记号的改变，结果方程 (8.5.112) $\sim$ (8.5.121) 可化成方程 $P_i=0$, P_i 由如下 (8.5.122) $\sim$ (8.5.131) 给出 (撇号表示相对于 t 求导):

$$P_1=x_{11}-x_{31}*x_{22}-x_{21}, \tag{8.5.122}$$

$$P_2=x_{31}^2+x_{32}^2-x_{11}^2, \tag{8.5.123}$$

$$P_3=x_{21}', \tag{8.5.124}$$

$$P_4=x_{22}', \tag{8.5.125}$$

$$P_5=x_{31}*x_{32}'-x_{32}*x_{31}'-x_{51}, \tag{8.5.126}$$

$$P_6=x_{51}', \tag{8.5.127}$$

$$P_7=x_{15}+x_{51}^2-x_{21}, \tag{8.5.128}$$

$$P_8 = (x''_{31})^2 + (x''_{32})^2 - x_{12}^2, \tag{8.5.129}$$

$$P_9 = 2 * x'_{11} * x_{12} + x_{11} * x'_{12}, \tag{8.5.130}$$

$$P_{10} = x_{31} * x''_{32} - x_{32} * x''_{31}. \tag{8.5.131}$$

现在取上面对应于 Kepler 定律集合中的微分多项式 (8.5.122)~(8.5.129) 组成微分多项式集 DPS. 我们要注意到行星在真正的非退化椭圆而非圆轨道上运行，所以有

$$\left.\begin{array}{ll} x_{21} = p \neq 0, & x_{22} = e \neq 0, \\ x_{11} = r \neq 0, & x'_{11} = r' \neq 0, \end{array}\right\} \tag{8.5.132}$$

且有

$$x_{15} = c \neq 0, \qquad x_{12} = A \neq 0. \tag{8.5.133}$$

在应用我们的算法寻找 DPS 的微分特征列 DCS 的过程中，我们可以去掉任何如上的因子. 最后得到的 DCS 为由 8 个微分多项式 C_i 组成的第 7 个微分基列，其指标集如下：

$$[7\ \ r^{(iv)}\ \ 1], [4\ \ A\ \ 2], [3\ \ c\ \ 1], [3\ \ p\ \ 1], [7\ \ e\ \ 2], [3\ \ x\ \ 1], [3\ \ y\ \ 2], [3\ \ h\ \ 1].$$

在这 8 个微分多项式 C_i 中，第一个只含有 $x_{11} = r$, 第二个含有 $x_{12} = A$. 第一个于是给我们一个半径向量 r 遵守的 4 阶导数微分方程. 这个方程和第二个关于 A 和 r 的方程都是太复杂了，因此无意义. 然而在计算过程中，第 4 个微分基列 DBS_4 由 6 个微分多项式 B_{4i} 组成，其中第一个 B_{41} 如下：

$$B_{41} = 2 * x_{12} * x'_{11} + x'_{12} * x_{11} = 2 * r' * A + r * A'.$$

根据我们的一般原理， $B_{41} = 0$ 是最初的微分多项式集的一个推论，也即 Kepler 定律的一个推论. 方程 $B_{41} = 0$ 恰恰就是 Newton 定律中的平方反比律 $r^2 * A = \text{const}$. 我们于是以自动的方式，用我们的一般原理从 Kepler 定律发现了 Newton 定律 (N_1). 进一步地，在计算过程中，第 3 个微分基列 DBS_3 由 6 个微分多项式 B_{3i} 组成，其中第一个 B_{31} 如下：

$$B_{31} = x_{15}^2 * x_{12}^2 * x_{11}^4 - 1 = c^2 * r^4 * A^2 - 1.$$

方程 $B_{31} = 0$ 也是 Kepler 定律的一个推论，它隐含着

$$c = \pm\frac{1}{r^2 * A}. \tag{8.5.134}$$

由 Newton 定律 (N_1) 知，比例常数 $r^2 * A$ 等于通用常数 c 的倒数，至多相差一个符号，因此它也是一个通用常数. Newton 定律 (N_3) 于是以自动的方式发现了.

(8.5.134) 中符号的不确定性是由于在 (8.5.119) 中引入加速度时只给出了大小而没有考虑方向. 如果我们取 $\sqrt{A^2}$ 的正值作为指向恒星的加速度向量 A, 那么 (8.5.134) 中就取正号 (+), 所以有

$$r^2 * A = +\frac{1}{c} = +\frac{h^2}{p}$$

是一个与行星无关的通用常数，尽管最后依赖于恒星.

我们现在假定两个物体 M 和 m 之间的吸引力与其质量 M 和 m 成正比. 按照 Newton 的动力学定律，物体 m 在外力 F 的作用下，将以 $F = m * A$ 给出的加速度 A 运动，那么我们可以立即从 Newton 定律 (N_1) ~ (N_3) 推导出如下的 Newton 万有引力定律.

在质量为 M 的恒星和质量为 m 的行星之间引力 F 为

$$F = G * \frac{M * m}{r^2},$$

其中 r 为恒星和行星之间的距离, G 为与行星无关的通用常数. 实际上，通用常数 G 与上面的 c 可通过关系式 $G = +\frac{1}{M*c}$ 联系起来，如果把恒星和行星放到对称的位置上来看, G 也应该是与恒星无关的常数.

注释 在上面的公式中，我们假定事先并不知道 Newton 万有引力定律，最后证明用我们的一般方法自动地发现了它. 上面的运算是在一台 SUN3/140 机器上进行的，耗时 15′58″, 且 $\max t = 342$, 其中 $\max t$ 是指计算过程中出现的微分多项式的项数的最大值. 在文章 [WWT32] 中试用了不同的坐标系和方程来做. 比较不同的试验可知，假定事先知道 Newton 定律用纯粹的力学方法证明要比事先不知道用自动发现的方法证明简单一些.

<u>一些进一步的补充和扩展</u>

无法把数学机械化中心成员及其合作者近几年来在数学机械化及相关领域的工作全部列出在这里. 下面仅给出他们的研究的题目的一个不完全列表，这里我们不给出参考文献，而将它们放在相关的文章中，主要放在了《数学机械化中心预印本》中.

下面是研究题目和作者的列表:

例证法，传统的和可读的证明, Clifford 代数技术 (洪加威，周咸青，高小山，张景中，杨路，程民德，李洪波等).

参数化和曲线同构 (高小山, 杜洪等).

一般代数系统, 实判别式系统, 不变量和协变量理论 (李连, 杨路, 侯晓荣, 邹丰美等).

解多项式方程组的特征值方法, 带有量词的线性系统 (吴文达, 黄玉珍, 冯果忱, 李连, 黄凯, 张树功等).

平面微分系统, 极限环, 稳定性 (王东明, 陆征一, S. L. Ma, S. C. Ning, S. M. Zhu, 刘卓军等).

微分系统, 偏微分方程, 混沌现象 (李子明, 李志斌, M. L. Wang, S. J. Wu, 张洪庆, J. Q. Fang 等).

统计力学中的杨 -Baxeter 方程, 量子群 (石赫, 吴可, 王世坤等).

编码和密码理论 (刘卓军, 杜洪等).

Stewart 平台问题, 弹性系统, 电工系统, spline 系统 (吴文达, 黄玉珍, 梁崇高, 陈陈, R. H. Wang, Y. S. Zhou 等).

控制论, 极点分配问题 (石赫, 李树荣).

计算机视觉, 数据压缩, 模式识别, 小波理论 (程民德, 石青云, C. X. Xu, W. W. Fang 等).

一阶逻辑的余式方法, 多值逻辑, 广义归纳法, 证明检验, probable inference, infinite logic (吴金昭, 刘卓军, X. H. Liu, 黄且园, 胡国定等).

参考文献

[A-H] Appel K. & Haken W., Every map is four colorable, Illinois J. Math., 21 (1977), 421-490, 491-567.

[Ak] Akritas A.G., Elements of Computer Algebra with Applications, John Wiley & Sons, 1989.

[Ar] Arnon D.S., A bibliography of quantifier elimination for real closed fields, J. Symb. Comp., 5 (1988), 267-274.

[A-M] Arnon D.S. & Mignotte M., On mechanical quantifier elimination for elementary algebra and geometry, J.Symb.Comp., 5 (1988), 237-260.

[Baj] Bajaj C.L., Surface fitting using implicit algebraic surface patches, in Curve and Surface Modelling (ed. H.Hagen), SIAM Publ. (1991), 1-31.

[B-I] Bajaj C.L. & Ihm I., Algebraic surface design with interpolation, ACM Trans. on Graphics, 19 (1992), 61-91.

[B-W] Becker T. & Weispfennig V., Groebner basis, Springer (1993).

[Bey] Beyer R.A., The kinematic synthesis of mechanisms, McGraw-Hill (1963).

[B-M] Blaschke W. & Mueller H.R., Ebene Kinematik, Muenchen (1956).

[B-L] Bledsoe W. W. & Loveland D.W. (Eds.), Automated theorem proving, after 25 Years, Amer.Math.Soc. (1984).

[Bo] Bocher M., Introduction to Higher Algebra, Macmillan, 1907.

[B-C-R] Bochnak J., Coste M. & Roy M-F., Géomètrie algébrique réelle, Springer (1986).

[B-S] Brasselet J.P. & Schwartz, M.H., Sur les classes de Chern d'un ensemble analytique complexe, Astéristique, $N^0$82-83 (1981).

[B-T] Brown W.S. & Traub J.F., On Euclid's algorithm and the theory of subresultants, J.ACM, 18 (1971), 505-514.

[Bu1] Buchberger B., Ein algorithmitisches Kriterium fuer die Loesbarkeit eines algebraishes Gleichungssystems, Aeq.Math, 4 (1970), 374-383.

[Bu2] Buchberger B., Some properties of Groebner bases for polynomial ideals, ACM SIGSAM Bull., 10 (1976), 19-24.

[BU3] Buchberger B., An algorithmic method in polynomial ideal theory, in N.K.Bose (Ed.), Recent Trends in Multidimensional Systems Theory, Reidel (1985), 184-232.

[B-L-C] Buchberger B., Loos R. & Collins G.E., Computer Algebra —— Symbolic and

Algebraic Computation, Springer Verlag (1982).

[Chern1] Chern S.S., On the characteristic classes of complex sphere bundles and algebraic varieties, J. Amer. Math. Soc., 75 (1953), 565-597.

[Chern2] Chern S.S., Characteristic classes of Hermitian manifolds, Annals of Math., 47 (1946), 88-121.

[Chou1] Chou S.C., Proving elementary geometry theorems using Wu's algorithm, in [B-L], 243-286.

[Chou2] Chou S.C., Proving and discovering geometry theorems using Wu's method, Ph.D Thesis, UTA (1985).

[Chou3] Chou S.C., Mechanical geometry theorem-proving, Reidel (1988).

[C-G] Chou S.C. & Gao X.S., On the mechanical proof of geometry theorems involving inequalities, Preprints TR-89-31, UTA (1989).

[C-G-M] Chou S.C., Gao X.S. & Mcphee N., A combination of Ritt-Wu's method and Collins' method, Preprint TR-89-28, UTA (1989).

[C-G-Z] Chou S.C., Gao X.S. & Zhang J.Z., Mechine proofs in geometry, World Scientific, Singapore (1994).

[C-S-Y] Chou S.C., Schelter W.F. & Yang J.G., An algorithm for constructing Groebner bases from characteristic sets and its applications to geometry, Algorithmica, 5 (1990), 147-154.

[Chow1] Chow W.L., Algebraic varieties with rational dissections, Proc. Nat. Acad. Sci., 42 (1956), 116-119.

[Chow2] Chow W.L., On the equivalence classes of cycles in an algebraic variety, Annals of Math., 64 (1956), 450-479.

[Ch-VdW] Chow W.L. & Van der Waerden, Ueber Zugeordnete Formen und algebraische Systeme von Mannigfaltigkeiten, Math. Ann., 113 (1937), 692-704.

[Col1] Collins G.E., Subresultants and reduced polynomial sequences, J.ACM, 14 (1967), 128-142.

[Col2] Collins G.E., Quantifier elimination for real closed fields: a guide to the literature, in [B-L-C], p.79-81.

[Col3] Collins G.E., Quantifier elimination for real closed fields by cylindrical algebraic decomposition, in 2nd GI Conf. Automata Theory & Formal Languages, Springer (1975), 134-183.

[C-H] Collins G.E. & Hong H., Partial cylindrical algebraic decomposition for quantifier elimination, J. Symb. Comp., 12 (1991), 299-328.

[Cou] Courant, R., Differential and Integral Calculus, vol.2, London & Glascow (1936).

[C-L-S] Cox D., Little J. & O'Shea D., Ideals, varieties, and algorithms, Springer (1992).

[C-G] Czapor S.R. & Geddes K.O., On implementing Buchberger's algorithm for Groebner basis, Proc. SYMSAC'86 (1986), 233-237.

[Dehn1] Dehn M., Ueber raumliche Polyeder, Nachr.Akad.Wiss.Goettingen, Math.-Phys.Kl. (1900), 345-354.

[Dehn2] Dehn M., Ueber der Raum Inhalt, Math.Ann., 55 (1902), 465-478.

[Eh] h Ehresmann C., Sur la topologie de certaines espaces homogènes, Ann. of Math., 35 (1934), 396-443.

[Eisb] Eisenbud D., Commutative algebra with a view toward algebraic geometry, Springer (1995).

[Eish] Eisenhart L.P., A treatise on the differential geometry of curves and surfaces (1909).

[F-W-Z] Feng G.C., Wu W.D. & Zhang S.G., The eigenvalue problem equivalent to multivariate polynomial system, MM-Res.Preprints, MMRC, 8 (1992), 134-142.

[Fr] Fricke R., Lehrbuch der Algebra, Bd 1 (1924).

[Gab] Gabriel J.R., SARA-A small automated reasoning assistant, Preprint, Argonne Nat. Lab. (1986).

[Gam] Gamkrelidze P.B., Chern cycles of complex algebraic manifolds, Izv. Acad. Scis., CCCP, math. ser., 20 (1956) 685-706 (in Russian).

[Gao1] Gao Xiao-shan, The discriminant systems of unary equations and their computation, MM-Res.Preprints, MMRC, No.1 (1987), 13-32.

[Gao2] Gao Xiao-shan, Constructive methods for polynomial sets and their applications, (in Chinese) PhD Thesis, Inst. of Systems Science, Acad. Sinica (1988).

[G-L-L-L] Gao X.S., Li Y., Lin D.D. & Liu X.S., A prover based on Wu's method, Proc.Intern.Workshop on Math.Mech. in Beijing, Intern.Acad.Publishers, Beijing (1992), 201-205.

[Gau1] Gauss C.F., Bestimmung der groessten Ellipse welche die vier Seiten eines gegebenen Vierecks beruehrt, Zach. Monatliche Correspondenz fuer Erd- und Himmelskunde, Bd 22 (1810), 112-121, or Werke, Bd.4 (1882) 385-392.

[Gau2] Gauss C.F., Das vollstaendige Fuenfeck und seine Dreiecke, Astro. Nachrichten, Nr.42 (1923), or Werke, Bd.4 (1882), 406-407.

[Gau3] Gauss C.F., Supplementum theorias combinations observationum erroribus minimis obnoxiae, in Werke, Bd 4 (1880), 8-93.

[Gre] Greenberg M.J., Euclidean and non-euclidean geometries, development and history, 2nd Ed., Freeman (1980).

[Gro] Groebner W., Moderne algebraische Geometrie, Springer (1949).

[G-L] Guan A.W. & Liu H.L., The machine proof of five positions plane rigid body guidance mechanism synthesis, Proc.ASCM'95 in Beijing, Scientists Incorporated, Tokyo (1995), 145-152.

[H-D] Hartenberg R.S. & Denavit J., Kinematic synthesis of linkages, McGraw-Hill (1964).

[Hen] Hensel K., Eine neue Theorie der algebraichen Zahlen, Math.Z., 2 (1918) 433-452.

[Her] Hermann G., Die Frage der endlich vielen Schritte in der Theorie der Polynomideale, Math.Ann., 95 (1925), 736-788.

[Hil1] Hilbert D., Grundlagen der Geometrie, Goettingen (1899).

[H-P1] Hodge W.V.D. & Pedoe D., Methods of algebraic geometry, vol.1, Cambridge (1947).

[H-P2] Hodge W.V.D. & Pedoe D., Methods of algebraic geometry, vol.2, Cambridge (1952).

[H-W] Hu S. & Wang D.M., Fast factorization of polynomials over rational number field or its extension fields, Kuxue Tongbao, 31 (1986), 150-156.

[H-WWD] Huang Y.Z. & Wu W.D., A modified version of an algorithm for solving multivariate polynomial systems, MM-Res.Preprints, MMRC, 5 (1990), 23-29.

[Jan] Janet M., Lecons sur les systèmes d'équations aux dérivées partièlles, Gauthier Villars (1920).

[Kal] Kalkbrehner M., A generalized Euclidean algorithm for computing triangular representations of algebraic varieties, J. Symb. Comp., 15 (1993), 143-167.

[Kap1] Kapur D., Using Gröbner bases to reason about geometry problems, J. Symb. Comp., 2 (1986), 399-408.

[Kap2] Kapur D., A refutional approach to geometry theorem proving, Art. Int., 37 (1988), 61-94.

[K-M] Kapur D. & Mundy J.L., Wu's method and its applications to perspective viewing, Art.Int., 37 (1988), 15-36.

[Kl] Klein F., Vorlesungen ueber nicht-Euklidische Geometrie (1927).

[Knu] Knuth D.E., The art of computer programming, v.2., Addison-Wesley (1969).

[K-F-F] Kobayashi H., Fujise T. & Furakawa A. Solving systems of algebraic equations by a general elimination method, J.Symb.Comp., 5 (1988), 303-320.

[Kol] Kolchin E.R., Differential algebra and algebraic groups, Academic Press (1973).

[Kr] Kronecker L., Grundzuege einer arithmetischen Theorie der algebraischen Groessen, J.f.Math., 92 (1882), 1-122.

[Ku] Ku Y.H., Note on a method of evaluating the complex roots of a quartic equation, J.Math. and Physics, Cambridge, Mass., 5 (1926), 126-128.

[K-S] Kutzler B. & S. Stifter, On the application of Buchberger's algorithm to automated geometry theorem proving, J.Symb.Comp., 2 (1986), 389-398.

[Laz1] Lazard D., Solving zero-dimensional algebraic systems, J.Symb.Comp., 13 (1992), 117-131.

[Laz2] Lazard D., A new method for solving algebraic systems of positive dimension, to be published in Discr.Appl.Math.

[Lef] Lefschetz S., Topology, Amer.Math.Soc.Coll.Publs. (1930).

[LHB1] Li H.B., New explorations on mechanical theorem proving of geometries, PhD Thesis, Beijing Univ., Beijing (1994).

[LHB2] Li H.B., Automated reasoning with differential forms, Proc.ASCM'95 in Beijing, Scientists Incorporated, Tokyo (1995) 29-32.

[L-C] Li H.B. & Cheng M.T., Proving theorems in elementary geometries with Clifford algebra method, to be published in Chinese Math. Progress.

[L-S] Li H.B. & Shi H., On Erdös′ ten point problem, MM-Res.Preprints, MMRC, 15 (1997) 53-63. Also in Acta Math. Sinica, New Ser., 13 (1997), 221-230.

[LTY] Li T.Y., Solving polynomial systems by homotopy continuation methods, Proc. Nankai on Computer Math. in 1991 Tianjin, World Sientific, Singapore (1993), 18-35.

[LXY] Li X.Y., Synthetic introduction to four-bar mechanism (in Chinese), Mech. Industry Press, Beijing (1965).

[LZB] Li Z.B., Wu method and solitons, Proc.ASCM′1995, Scientists Incorporated, Tokyo (1995), 157-164.

[Li-Ch] Li Z.B. & Chen S.K., Finding solitary wave solutions of non-linear wave equations using symbolic computation, Proc. ASCM'96 in Kobe, Scientific Incorporated, Tokyo (1996), 63-72.

[LZM1] Li Z.M., A new proof of Collins's theorem, MM-Res.Preprints, MMRC, No.1 (1987), 33-37.

[LZM2] Li Z.M., On the trianguration for any finite polynomial set (I), MM-Res. Preprints, MMRC, No.2 (1987), 48-54

[LZM3] Li Z.M., Determinant polynomial sequences, MM-Res.Preprints, MMRC, No.3 (1989), 51-55.

[Liang] Liang C.G., Input-output equation of 7R mechanism and inverse solution of general 6R manipulator, Proc.1992 Intern.Workshop on Math.Mech., (Eds. W.T.Wu

& M.D.Cheng), Intern.Acad.Publishers, Beijing (1992), 189-200.

[L-L] Lin D.D. & Liu Z.J., Some results on theorem proving in finite geometry, Proc.1992 Intern.Workshop on Math.Mech. in Beijing, Intern.Acad.Publishers, Beijing (1992), 222-235.

[LXF1] Liu X.F., Singularities of algebraic varieties, PhD Thesis, Eastern China Normal Univ., Shanghai (1995).

[LXF2] Liu X.F., The genera of algebraic curves with singularities, Proc.ASCM'95, Beijing (1995), 23-28.

[Liu] Liu Z.J., Mechanical approach for deciding the construction of system equations' solutions and its related problems (in Chinese) PhD Thesis, Inst. of Systems Science, Beijing (1988).

[Lyon] Lyon W.V., Note on a method of evaluating the complex roots of a quartic equation, J.Math. and Physics, Cambridge, Math., 3 (1924).

[Mac] Macaulay F.S., Some properties of enumeration in the theory of modular systems, Proc.London Math.Soc., 26 (1927), 531-555.

[MP] MacPherson R.D., Chern classes for singular algebraic varieties, Ann. of Math., 100 (1974), 423-432.

[Mig] Mignotte M., Computer versus paper and pencil, Proc. CALSIF 4 (1986) 63-69. Also in Proc.Nankai on Comp.Math. in 1991 Tianjin, World Scientific, Singapore (1993), 112-117.

[Miy] Miyaoka Y., On the Chern numbers of surfaces of general type, Invent. Math., 42 (1977), 225-237.

[Mou] Moulton F.R., The straight line solutions for the problem of n-bodies, Ann. of Math., 12 (1910), 1-17.

[O1] Ostrowski, A.M., Solution of equations and systems of equations, Acad.Press (1960).

[O2] Ostrowski A.M., Recherches sur la méthode de Graeffe et les zeros des polynomes et des series de Laurent, Acta Math., 72 (1940), 99-155.

[Paul] Paul R.P., Robot manipulators: Mathematics, programming, and control, MIT Press (1981).

[Pet] Petersen J., Die Steinersche Loesung der Malfattischen Aufgabe, J.f.Math. 89 (1880), 127-135.

[Riq] Riquier C.H., La méthode des fonctions majorantes et les systèmes d'équations aux dérivées partièlles, Gauthier Villars (1928).

[Ritt1] Ritt J.F., Differential equations from the algebraic standpoint, Amer. Math.

Soc. (1932).

[Ritt2] Ritt J.F., Differential algebra, Amer.Math.Soc. (1950).

[S-S-K-S] Sasaki T., Suzuki M., Kolar M. & M. Sasaki, Approximate factorization of multivariate polynomials and absolute irreducibility testing, Japan J.Ind.Appl.Math., 8 (1991), 359-375.

[S-R] Semple J.G. & Roth L., Introduction to algebraic geometry, Oxford (1949).

[Shi1] Shi H., On Chern characters of algebraic hypersurfaces with arbitrary singularities, Acta Math.Sinica, New Ser., 4 (1988), 289-300.

[Shi2] Shi H., Chern classes of algebraic varieties with singularity, Singularity theory, World Scientific, Singapore (1995), 705-730.

[Sm1,2] Smale S., Topology and mechanics, I, II, Invent. Math., 10 (1970), 305-331; 11 (1970), 45-64.

[St] Steiner J., Geometrische Betrachtungen, J.f.Math., 1 (1826), 178-180.

[Syd] Sydler J.P., Conditions nécèssaires et suffisantes pour l'équivalence des polyédres de l'espace euclidien à trois dimensions, Comm.Math.Helv., 40 (1965), 436-480.

[Syn] Synge J.L., On the motion of three vortices, Canad.J.Math., 1 (1949), 257-270.

[Tai] Tai S.S., A class of symmetric functions and Chern numbers of algebraic varieties, Lect.Notes in Math., No.1369, Springer (1989), 261-274.

[Tar] Tarski A., A decision method for elementary algebra and geometry, 2nd Edn., Univ.Calif.Press, Berkeley (1951).

[Th1] Thomas J.M., Differential systems, Amer.Math.Soc. (1937).

[Th2] Thomas J.M., Riquier's existence theorems, Annals of Math., 30 (1929), 286-310; 35 (1934), 306-311.

[Todd] Todd J.A., The geometrical invariants of algebraic loci, Proc. London Math. Soc. (2), 43 (1937), 127-138.

[Tr] Traeger B.M., Algebraic factoring and rational function integration, Proc. 1976 ACM Symp. Symb. and Alg. Comp. (1976), 219-226.

[VdV] Van de Ven, On the Chern numbers of surfaces of general type, Invent. Math., 36 (1976), 285-293.

[VdW1] Van der Waerden, Moderne Algebra, Teil 1 (1930), Teil 2 (1931).

[VdW2] Van der Waerden, Einfuerung in die algebraischen Geometrie, Dover Publ. (1945).

[Wald] Waldvogel J., Note concerning a conjecture by A.Wintner, Celestial Mechanics, 5 (1972), 37-40.

[Wall] Wall B., On the computation of syzygies, ACM SIGSAM Bull., 23 (1989), 5-14.

[Wan] Wan Z.X., Geometry of classical groups over finite fields, Studentliteratur, Lund (1993).

[WDK1] Wang D.K., A mechanization proving of a group of space geometry problems, MM-Res.Preprints, MMRC, No.5 (1990), 66-81.

[WDK2] Wang D.K., Polynomial equations solving and mechanical geometric theorem proving, PhD.Thesis, MMRC (1993).

[WDM1] Wang D.M., Mechanical approach for polynomial set and its related fields (in Chinese), Ph.D thesis, Inst.Sys.Sci. (1987).

[WDM2] Wang D.M., On Wu's method for proving constructive geometric theorems, MM-Res.Preprints, MMRC, No.3 (1989), 89-101.

[WDM3] Wang D.M., A new theorem discovered by computer prover, Journal of Geometry, 36 (1989), 173-182.

[WDM4] Wang D.M., A method for factoring multivariate polynomials of successive algebraic-extension fields, Preprint, RISC-LINZ Johannes Kepler University, Australia (1995).

[WDM5] Wang D.M., A decision method for definite polynomial, MM-Res. Preprints, MMRC, No.2 (1987), 68-74.

[W-G] Wang D.M. & Gao X.S., Geometry theorems proved mechanically using Wu's method — Part on Euclidean geometry, in MM-Res.Preprints, MMRC, No.2 (1987), 75-106.

[WH1] Wang H., Toward mechanical mathematics, IBM Journal, 4 (1960), 2-22.

[WH2] Wang H., A survey of mathematical logic, Science Press, Beijing (1962).

[WPS1] Wang P.S., Factoring multivariate polynomials over algebraic number fields, Math. Comp., 30 (1976), 324-336.

[WPS2] Wang P.S., An improved multivariate polynomial factoring algorithm, Math. Comp., 32 (1978), 1215-1231.

[W-R] Wang P.S. & Rothschild L.P., Factoring multivariate polynomials over the integers, Math.Comp., 29 (1975), 935-950.

[Weil] Weil A., Foundations of algebraic geometry, Amer.Math.Soc. Colloq.Publ., 29 (1962).

[Whit] Whitney H., Elementary structure of real algebraic varieties, Annals of Math., 66 (1957), 545-556.

[Wint] Wintner A., Analytic foundations of celestial mechanics (1941).

[W-L] Wu J.Z. & Liu Z.J., On first order theorem proving, Proc. ASCM'96 in Kobe, Scientists Incorporated, Tokyo (1996), 163-186.

[WTJ1] Wu T.J., Some test problems on applications of Wu's method in nonlinear programming problems, MM-Res. Preprints, MMRC, No.6 (1991), 144-155. Also in Ch.Q.J.Math., 9 (1994), 8-17.

[WTJ2] Wu T.J., On a collision problem, MM-Res. Preprints, MMRC, No.7 (1992) 96-104. Also in Acta Math.Scientia, 15 (Supp.) (1995), 32-38.

[WWD] Wu W.D., A note to the discriminant systems for the unary equations, MM-Res.Preprints, MMRC, No.3 (1989), 33-38.

[WWT1] Wu W.T., On the decision problem and the mechanization of theorem-proving in elementary geometry, Scientia Sinica, 21 (1978), 159-172, re-published in [B-L] (1984), 235-242.

[WWT2] Wu W.T., Toward mechanization of geometry — Some comments on Hilbert's "Grundlagen der Geometrie", Acta Math.Scientia, 2 (1982), 125-138

[WWT3] Wu W.T., Some remarks on mechanical theorem-proving in elementary geometry, Acta Math.Scientia, 3 (1983), 357-360.

[WWT4] Wu W.T., Some recent advance in mechanical theorem-proving of geometries, in [B-L] (1984), 235-242.

[WWT5] Wu W.T., Basic Principles of Mechanical Theorem Proving in Geometries (Part on Elementary Geometries) (in Chinese), Science Press (1984). English translation by D.M.Wang et al, Springer (1994).

[WWT6] Wu W.T., Basic principles of mechanical theorem-proving in elementary geometries, J.Sys.Sci. & Math.Scis., 4 (1984), 207-235. Re-published in J. of Automated Reasoning, 2 (1986), 221-252.

[WWT7] Wu W.T., On zeros of algebraic equations — an application of Ritt principle, Kexue Tongbao, 31 (1986), 1-5.

[WWT8] Wu W.T., A mechanization method of geometry and its applications, I. Distances, areas, and volumes, J.Sys.Sci. & Math.Scis.,6 (1986), 204-216.

[WWT9] Wu W.T., A mechanization method of geometry and its applications, I. Distances, areas, and volumes in euclidean and non-euclidean geometries, Kuxue Tongbao, 32 (1986), 436-440.

[WWT10] Wu W.T., A zero structure theorem for polynomial-equations-solving and its applications, MM-Res.Preprints, MMRC, No.1 (1987), 2-12.

[WWT11] Wu, W.T., A mechanization method of geometry and its applications, 3. Mechanical proving of polynomial inequalities and equations-solving, MM-Res. Preprints, MMRC, No.2 (1987), 1-17.

[WWT12] Wu W.T., A mechanization method of geometry and its applications, 4. Some

theorems in planar kinematics, J.Sys.Scis & Math.Sci., 2 (1989), 97-109.

[WWT13] Wu W.T., Some remarks on characteristic-set formation, MM-Res. Preprints, MMRC, No.3 (1989), 27-29.

[WWT14] Wu W.T., On the generic zero and Chow basis of an irreducible ascending set, MM-Res. Preprints, MMRC, No.4 (1989), 1-21.

[WWT15] Wu W.T., On the chemical equilibrium problem and equations-solving, MM-Res. Preprints, MMRC, 4 (1989), 22-39. Also in Acta Math.Sci., 10 (1990), 361-374.

[WWT16] Wu W.T., On a projection theorem of quasi-varieties in elimination theory, MM-Res.Preprints, MMRC, No.4 (1989), 40-48. Also in Chin.Ann. of Math., 11B (1990), 220-226.

[WWT17] Wu W.T., A mechanization method of geometry and its applications, 6. Solving inverse kinematic equations of Puma-type robots, MM-Res.Preprints, MMRC, 4 (1989), 49-53.

[WWT18] Wu W.T., On the construction of Groebner basis of a polynomial ideal based on Riquier-Janet theory, MM-Res.Preprints, MMRC, No.5 (1990), 5-22. Also in Sys.Sci.& Math.Scis., 4 (1991), 193-207.

[WWT19] Wu W.T., On a linear equations method of non-linear polynomial equations-solving, MM-Res.Preprints, MMRC, No.6 (1991), 23-36. Also in Sys.Sci. & Math.Scis., 6 (1993), 1-12.

[WWT20] Wu W.T., Equations-solving and theorem-proving: Zero-set formulation and ideal formulation, Proc.Asian Math.Conf.1990 in Hongkong (1992), 1-10.

[WWT21] Wu W.T., A mechanization method of equations-solving and theorem- proving, Adv.in Comp. Res., 6 (1992), 103-138.

[WWT22] Wu W.T., On problems involving inequalities, MM-Res.Preprints, MMRC, No.7 (1992), 1-13.

[WWT23] Wu W.T., On a finiteness theorem about optimization problems, MM-Res.Preprints, MMRC, No.8 (1992), 1-18.

[WWT24] Wu W.T., A report on mechanical geometry theorem proving, Progress in Natural Science, 2 (1992), 1-17.

[WWT25] Wu W.T., On a hybrid method of polynomial equations solving, MM-Res.Preprints, MMRC, No.9 (1993), 1-10.

[WWT26] Wu W.T., On surface-fitting problem in CAGD, MM-Res. Preprints, MMRC, No.10 (1993), 1-10.

[WWT27] Wu W.T., On a finiteness theorem about problems involving inequalities,

Sys.Sci. & Math.Scis., 7 (1994), 193-200.

[WWT28] Wu W.T., Some remarks on factorization and GCD of multivariate polynomials, MM-Res.Preprints, MMRC, No.11 (1994), 1-14.

[WWT29] Wu W.T., Polynomial equations-solving and its applications, Proc. ISAAC'94, or Algorithm and Computations, (Eds. D.Z.Du & X.S.Zhang), Springer (1994), 1-9.

[WWT30] Wu W.T., Central configurations in planet motions and vortex motions, MM-Res. Preprints, MMRC, No.13 (1995), 1-14.

[WWT31] Wu W.T., A mechanization method of geometry and its applications, 2. Curve pairs of Bertrand type, Kexue Tongbao, 32 (1987), 585-588.

[WWT32] Wu W.T., Mechanical derivation of Newton's gravitational laws from Kepler's laws, MM-Res.Preprints, MMRC, No.1 (1987), 53-61.

[WWT33] Wu W.T., On the foundation of algebraic differential geometry, MM-Res.Preprints, MMRC, No.3 (1989), 1-26.

[WWT34] Wu W.T., Mechanical theorem-proving of differential geometries and some of its applications in mechanics, J.Aut.Reasoning, 7 (1991), 171-191.

[WWT35] Wu W.T., On Chern characteristic systems of an algebraic variety, (in Chinese) Advances in Mathematics, 8 (1965), 395-401.

[WWT36] Wu W.T., On algebraic varieties with dual rational dissections, (in Chinese) Advances in Mathematics, 8 (1965), 402-409.

[WWT37] Wu W.T., On Chern numbers of algebraic varieties with arbitrary singularities, Acta Math. Sinica, New Series, 3 (1987), 227-236.

[W-L] Wu W.T. & Lu X.L., Triangles with equal bisectors, (in Chinese), People's Edu.Press, Beijing (1986).

[W-W] Wu W.T. & Wu T.J., A mechanization method of geometry and its applications, 5. Solving transcendental equations by algebraic methods, MM-Res.Preprints, MMRC, No.3 (1989), 30-32.

[Yau] Yau S.T., Calabi's conjecture and some new results in algebraic geometry, Proc. Nat. Acad. Sci., 74 (1977), 1798-1799.

[Y-H-Z] Yang L., Hou X.R. & Zeng Z.B. An alternative algorithm for determining the number of real roots of a polynomial, Intern.Workshop on Logic and software Engineering, Beijing (1995).

[Y-Z-H] Yang L., Zhang J.Z. & Hou X.R. Nonlinear algebraic equation system and automated theorem-proving (in Chinese), Shanghai Sci. and Tech.Edu.Publ.House, Shanghai (1996).

[ZSQ] Zhang S.Q., Wu elimination and its application in partial differential equations. Solitary wave solutions for non-linear evolution equations using symbolic computation, PhD Thesis, Lanzhou Univ., Lanzhou (1995).

[Zhi] Zhi L.H., Polynomial factorization over algebraic fields and applications, PhD. Thesis, MMRC (1996).

[Zhou] Zhou J.Y., Classes de Chern pour les variétès singulières. Classes de Chern en théorie bivariant, PhD Thesis, Marseille (1995).

[Zou] Zou F.M., Applications of the characteristic set method in celestial motions and invariant theory, PhD Thesis, MMRC (1997).

(O-1671.0101)
● 责任编辑：吕　虹
● 封面设计：黄华斌

数学机械化丛书（部分书目）

- 数学机械化　吴文俊
- 几何定理机器证明的几何不变量方法　张景中、高小山、周咸青
- 消去法及其应用　王东明
- 组合恒等式的机器证明　陈永川
- 几何自动作图与智能CAD　高小山
- 代数曲面造型　陈发来 等
- 非线性数学物理方程的行波解　李志斌 等



ISBN 7-03-010764-0
定 价：58.00元